

【TITLE OF THE INVENTION】

鍵共有システム、共有鍵生成装置及び共有鍵復元装置

KEY AGREEMENT SYSTEM, SHARED-KEY GENERATION APPARATUS, AND
SHARED-KEY RECOVERY APPARATUS

【BACKGROUND OF THE INVENTION】

【(1) Field of the Invention】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、第三者に知られることなく、鍵を配送する技術に関する。

【(2) Description of the Related Art】

従来より、送信装置から受信装置へ情報を秘密に送信するために、公開鍵暗号方式が用いられる。

公開鍵暗号方式では、送信装置は、通信内容を受信装置の公開鍵を用いて暗号化して送信し、受信装置は、暗号化された通信内容を受信し、受信した通信内容を自身の秘密鍵を用いて復号して元の通信内容を得る。(例えば、非特許文献1参照)。

1996年、高速処理が可能な公開鍵暗号として、NTRU暗号が提案された(例えば、非特許文献2参照)。NTRU暗号では、高速に演算可能な多項式演算を用いて暗号化と復号化とを行うので、べき乗演算を行うRSA暗号や楕円曲線上の点のスカラ倍演算を行う楕円曲線暗号と比較すると、これら従来の公開鍵暗号よりもソフトウェアにより高速に処理することが可能である。

しかし、このNTRU暗号では、公開鍵を用いて平文を暗号化して暗号文を生成し、正規の秘密鍵を用いて暗号文を復号して復号文を生成する際に、復号文が元の平文と異なる場合が発生する。このことを復号エラーが発生するという。なお、復号エラーを回避する方法として、平文に付加情報を付加して暗号化し、平文のハッシュ関数値と共に送信する方法が開示されている(例えば、特許文献1参照)。

一方で、近年、公開鍵暗号の新しい概念として、鍵カプセル化メカニズム(Key Encapsulation Mechanisms)と呼ばれる方式が提案されている(例えば、非特許文献3参照)。この鍵カプセル化メカニズムは、公開鍵暗号を用いて送信装置と受信装置との間で共有鍵を配送するアルゴリズムであり、送信装置は、暗号化アルゴリズムEに受信者の公開鍵 p_k を入力して暗号文Cと共有鍵Kを生成し、暗号文Cを受信装置に伝送する。次に、受信装置は、復号アルゴリズムDに、秘密鍵 s_k と暗号文Cを入力して送信装置と同じ共有鍵Kを求める。

このようにして鍵カプセル化メカニズムを用いて共有鍵Kを送信装置と受信装置とで共有した後に、送信装置は、受信装置へ送信すべき平文を、共有鍵Kを用いて共通鍵暗号方式に

より暗号化して暗号文を生成し、生成した暗号文を受信装置へ送信する。受信装置は、暗号文を受信し、受信した暗号文を共有鍵 K を用いて前記共通鍵暗号方式により復号して復号文を生成する。

鍵カプセル化メカニズムでは、送信者から受信者に一方的に情報の送信が行われていながら、送信者が作為的に共有鍵を作成できず、送信者による不正が抑制されている点が従来にない特徴である。

このような鍵カプセル化メカニズムとして、PSEC-KEMと呼ばれるアルゴリズムが開示されている（例えば非特許文献3、非特許文献4参照）。以下に、非特許文献4に記載されているPSEC-KEMアルゴリズムについて説明する。

(1) PSEC-KEMのシステムパラメータ

PSEC-KEMは、以下のシステムパラメータを持つ。

- ・楕円曲線： E
- ・楕円曲線上の位数 n の点： P
- ・ハッシュ関数： G 、 H

なお、楕円曲線、位数及びハッシュ関数については、非特許文献1に詳細が記述されているので、ここでは説明を省略する。

(2) PSEC-KEMの公開鍵と秘密鍵

- ・ランダムに Z_n の要素 x を選び、 $W = x * P$ を生成する。

ここで、 Z_n は、 $\{0, 1, \dots, n-1\}$ からなる集合であり、 $x * P$ は、楕円曲線上の点 P を x 個、加算することにより得られる楕円曲線上の点を表す。なお、楕円曲線上の点の加算方法については、非特許文献1に記述されている。

- ・公開鍵 p_k を (E, P, W, n) とし、秘密鍵 s_k を x とする。

(3) PSEC-KEMの暗号化

暗号化時には、以下に述べる暗号化アルゴリズム $KemE$ に公開鍵 p_k を入力して共有鍵 K と暗号文 C を出力する。以下に暗号化アルゴリズム $KemE$ について説明する。

- ・ハッシュ関数 H の出力ビット長と同じ長さの s をランダムに生成する。
- ・ $G(s)$ を生成し、 $G(s)$ を分割して、 a と K とを生成する。 a は、 $G(s)$ の上位複数ビットからなるビット列であり、 K は、残りのビットからなるビット列である。ここで、 $G(s) = a || K$ である。「 $||$ 」は、ビット結合を表す演算子である。つまり、 a と K とを結合すると、 $G(s)$ が得られる。
- ・ $R = a * P$ 、 $Q = a * W$ を生成する。
- ・ $v = s \text{ xor } H(R || Q)$ を生成する。ここで、 xor は排他的論理和演算を表す。
- ・共有鍵 K と暗号文 $C = (R, v)$ を出力する。

(4) PSEC-KEMの復号化

復号化時には、以下に述べる復号アルゴリズムK_{emD}に暗号文 $C = (R, v)$ と公開鍵 p_k と秘密鍵 s_k を入力して共有鍵 K を出力する。以下に復号アルゴリズムK_{emD}について説明する。

- ・ $Q = x * R$ を生成する。
- ・ $s = v \text{ xor } H(R || Q)$ を生成する。
- ・ $G(s)$ を生成し、 $G(s)$ を $G(s) = a || K$ と分割する。
- ・ $R = a * P$ が成立するかどうかチェックする。成立すれば共有鍵 K を出力する。

このPSEC-KEMアルゴリズムを、送信装置と受信装置の間で暗号化通信を行う暗号システムに適用する場合、まず、送信装置は、通信先受信装置の公開鍵 p_k を取得し、取得した公開鍵 p_k を前述の暗号化アルゴリズムK_{emE}に入力して共有鍵 K と暗号文 C を導出して、暗号文 C を受信装置へ送信する。

次に、受信装置は、送信装置から暗号文 C を受信し、受信した暗号文 C と自身が有する公開鍵 p_k ・秘密鍵 s_k を前述の復号アルゴリズムK_{emD}に入力して、送信装置が導出したものと等しい共有鍵 K を導出する。

以下に、さらに詳細に説明する。

今、PSEC-KEMアルゴリズムは、ハッシュ関数 H の入力を $(a * P || a * W)$ としており、暗号化アルゴリズムK_{emE}で、ランダムに生成した要素 s に $H(a * P || a * W)$ の値を作用させて v を生成する。そして、復号アルゴリズムK_{emD}では、 $R = a * P$ から秘密鍵 $s_k (= x)$ を用いて $Q = x * R = x * (a * P) = a * (x * P) = a * W$ を求めることができるので、 v に $H(a * P || a * W)$ の値を作用させて、暗号化アルゴリズムK_{emE}において生成されたランダムな要素 s を求めることができる。

従って、暗号化アルゴリズムK_{emE}と復号アルゴリズムK_{emD}は、ハッシュ関数 G に同じ s の値を入力することができ、同じ共有鍵 K を導出することができる。この結果、秘密鍵 s_k を有する受信装置は、送信装置が導出したものと同じ共有鍵 K を導出できることになる。

一方で、秘密鍵 s_k を知らない他の受信装置は、たとえ公開鍵 p_k を取得して暗号文 C を受信したとしても、秘密鍵 $s_k (= x)$ を知らないので $R = a * P$ から $Q = a * W (= (a * x) * P)$ を計算できず、送信装置が導出したものと同じ共有鍵 K を導出できない。

なぜならば、秘密鍵 s_k を知らない他の受信装置は、公開鍵 p_k しか利用できないので、上記 Q の計算には秘密鍵 $s_k (= x)$ の代わりに公開鍵 p_k の $W = x * P$ を利用することになるが、一般に、 $a * P$ と $W = x * P$ から、 $Q = a * W (= (a * x) * P)$ を求めることは、楕円曲線上のDiffie-Hellman問題と呼ばれ、 a や x の値を知らない限り計算困難だからである（例えば、非特許文献5参照）。

すなわち、PSEC-KEMアルゴリズムは、秘密鍵を用いずに $a * P$ から $a * W$ を計算することが困難な Diffie-Hellman 問題を用いて、最終的に共有鍵 K を導出することにより、秘密鍵を知らなければその共有鍵 K を導出できないようにしている。

以上により、送信装置と受信装置とは、共有鍵 K を秘密に共有することができ、この後、秘密鍵暗号を用いて、送信装置から受信装置へ通信される通信内容データを、共有鍵 K を用いて共通鍵暗号で暗号化する。

(特許文献1)

特開2002-252611号公報

(非特許文献1)

岡本龍明、山本博資、「現代暗号」、シリーズ／情報科学の数学、産業図書、1997.

(非特許文献2)

Jeffery Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998.

(非特許文献3)

Victor Shoup, "A proposal for an ISO standard for public key encryption (version 2.1)", [online], 2001年12月20日、[2002年9月29日検索]、インターネット<URL: http://shoup.net/papers/iso-2_1.pdf>

(非特許文献4)

Tatsuaki Okamoto, "Generic conversions for constructing IND-CCA2 public-key encryption in the random oracle model", [online], The 5th Workshop on Elliptic Curve Cryptography(ECC 2001)、2001年10月30日、[2002年9月29日検索]、インターネット<URL: <http://www.cacr.math.uwaterloo.ca/conferences/2001/ecc/okamoto.ppt>>

(非特許文献5)

Neal Koblitz, "Algebraic Aspects of Cryptography", Algorithms and Computation in Mathematics Vol.3, pp.132-133, Springer-Verlag, 1998.

(発明が解決しようとする課題)

上述したように、従来のPSEC-KEMアルゴリズムは、ハッシュ関数 H の入力に $a * P$ 、 $a * W$ を用い、秘密鍵を用いずに $a * P$ から $a * W$ を計算することが困難な Diffie-Hellman 問題を用いて、最終的に共有鍵 K を導出することにより、秘密鍵を知らなければその共有鍵 K を導出できないようにしている。

しかしながら、NTRU暗号をはじめ、Diffie-Hellman 問題を利用しない他の公開鍵暗号には、Diffie-Hellman 問題の $a * P$ 、 $a * W$ に相当するもの

がないため、PSEC-KEMアルゴリズムを適用できない。すなわち、高速処理が可能なNTRU暗号は、鍵カプセル化メカニズムであるPSEC-KEMアルゴリズムを適用して共有鍵の配送を行うことができず、従って、送信装置と受信装置とは、その共有鍵を用いた送信装置から受信装置への暗号化通信ができないという問題点がある。

【SUMMARY OF THE INVENTION】

そこで、本発明は上記の問題点を解決するために、Diffie-Hellman問題を利用しない暗号化方式を用いる場合であっても、共有鍵生成装置から共有鍵復元装置へ第三者に知られることなく共有鍵を配送し、この際に、共有鍵生成装置と共有鍵復元装置との間で異なる共有鍵が導出されるのを防止できる鍵共有システム、共有鍵生成装置、共有鍵復元装置、共有鍵生成方法、共有鍵復元方法、共有鍵生成プログラム及び共有鍵復元プログラムを提供することを目的とする。

上記目的を達成するために、本発明は、第3者に知られることなく共有鍵を生成する共有鍵生成装置及び共有鍵復元装置から構成される鍵共有システムであって、前記共有鍵生成装置は、シード値を生成するシード値生成手段と、生成された前記シード値から検証値及び共有鍵を生成する第1共有鍵生成手段と、生成された前記検証値を暗号化して、第1暗号化情報を生成する第1暗号化手段と、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第2暗号化情報を生成する第2暗号化手段と、生成された前記第1暗号化情報及び前記第2暗号化情報を送信する送信手段とを備え、前記共有鍵復元装置は、前記第1暗号化情報及び前記第2暗号化情報を受信する受信手段と、受信された前記第1暗号化情報を復号して第1復号検証値を生成する第1復号手段と、生成された前記第1復号検証値に基づいて、受信された前記第2暗号化情報を復号して、復号シード値を生成する第2復号手段と、前記第1共有鍵生成手段と同一の方法により、生成された前記復号シード値から第2復号検証値及び復号共有鍵を生成する第2共有鍵生成手段と、生成された前記第1復号検証値及び前記第2復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断手段と、出力すると判断される場合に、生成された前記復号共有鍵を出力する出力手段とを備える。

この構成によると、前記共有鍵生成装置は、シード値から検証値及び共有鍵を生成し、前記検証値を暗号化して第1暗号化情報を生成し、前記検証値に基づいて、前記シード値を暗号化して第2暗号化情報を生成し、前記共有鍵復元装置は、前記第1暗号化情報を復号して第1復号検証値を生成し、前記第1復号検証値に基づいて、前記第2暗号化情報を復号して、復号シード値を生成し、前記共有鍵生成装置と同様にして、前記復号シード値から第2復号検証値及び復号共有鍵を生成し、生成された前記第1復号検証値及び前記第2復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断するので、共有鍵生成装置か

ら共有鍵復元装置へ第三者に知られることなく共有鍵を配送できると共に、この際に、共有鍵生成装置と共有鍵復元装置との間で異なる共有鍵が導出されるのを防止できるという効果がある。

ここで、前記共有鍵生成装置は、さらに、コンテンツを取得する取得手段と、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成する暗号化手段とを備え、前記送信手段は、さらに、生成された前記暗号化コンテンツを送信し、前記受信手段は、さらに、前記暗号化コンテンツを受信し、前記共有鍵復元装置は、さらに、出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成する復号手段と、生成された復号コンテンツを出力する出力手段とを備える。

この構成によると、共有鍵生成装置は、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成し、前記共有鍵復元装置は、出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成するので、第三者に知られることなく、共有鍵生成装置から共有鍵復元装置へコンテンツを送信することができるという効果がある。

また、本発明は、第3者に知られることなく共有鍵を相手の装置へ伝える共有鍵生成装置であって、シード値を生成するシード値生成手段と、生成された前記シード値から検証値及び共有鍵を生成する共有鍵生成手段と、生成された前記検証値を暗号化して、第1暗号化情報を生成する第1暗号化手段と、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第2暗号化情報を生成する第2暗号化手段と、生成された前記第1暗号化情報及び前記第2暗号化情報を送信する送信手段とを備える。

この構成によると、共有鍵生成装置は、検証値を暗号化して第1暗号化情報を生成し、前記検証値に基づいて、シード値を暗号化して第2暗号化情報を生成するので、二重の暗号化により、より安全性を高めることができるという効果がある。不正な第三者は、第1及び第2暗号化手段による2種の暗号化を知っていなければ、共有鍵を得ることはできない。

ここで、前記シード値生成手段は、乱数を生成し、生成した乱数を前記シード値とすることにより、前記シード値を生成する。

この構成によると、共有鍵生成装置は、乱数を生成し、生成した乱数を前記シード値とするので、シード値を生成し、検証値及び共有鍵を生成し、第1暗号化情報及び第2暗号化情報を生成し、第1暗号化情報及び第2暗号化情報を送信した後、次に、シード値を生成する際に、最初に生成されたシード値とは異なるように、後のシード値を生成することができる。従って、共有鍵生成装置により送信される第1暗号化情報及び第2暗号化情報は、毎回異なるものとなる。このため、不正な第三者が、共有鍵生成装置から相手の装置へ送信される第1暗号化情報及び第2暗号化情報をその都度、盗聴し、記録したとしても、記録している各第1暗号化情報及び第2暗号化情報から元のシード値を類推することは困難である。

ここで、前記共有鍵生成手段は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値及び前記共有鍵を生成する。

この構成によると、前記シード値に一方向性関数を施して、前記検証値を生成するので、前記検証値を第三者が知り得たとしても、前記検証値から前記シード値を求めることは困難である。このため、前記検証値からシード値を求め、さらに、共有鍵を求めることは事実上不可能である。

ここで、前記共有鍵生成手段は、前記シード値に、前記一方向性関数として、ハッシュ関数を施して前記関数値を生成する。

この構成によると、前記一方向性関数は、ハッシュ関数であるので、その演算アルゴリズムがよく知られており、適用が容易である。

ここで、前記共有鍵生成手段は、生成された前記関数値の一部を前記検証値とし、他の一部を前記共有鍵とすることにより、前記検証値及び前記共有鍵を生成する。

この構成によると、前記関数値の一部を前記検証値とし、他の一部を前記共有鍵とすることで、前記検証値及び前記共有鍵の生成が容易である。

ここで、前記共有鍵生成手段は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値、前記共有鍵及びブラインド値を生成する。

この構成によると、前記シード値に一方向性関数を施して、前記検証値を生成するので、前記検証値を第三者が知り得たとしても、前記検証値から前記シード値を求めることは困難である。このため、前記検証値からシード値を求め、さらに、共有鍵を求めることは事実上不可能である。

ここで、前記第1暗号化手段は、公開鍵を取得する公開鍵取得部と、取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第1暗号化情報を生成する公開鍵暗号化部を含む。

また、前記第1暗号化手段は、公開鍵を取得する公開鍵取得部と、取得された前記公開鍵を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第1暗号化情報を生成する公開鍵暗号化部を含む。

この構成によると、第1暗号化手段は、公開鍵暗号方式を用いるので、共有鍵暗号方式を用いる場合と比較すると、鍵の管理が容易である。

ここで、前記公開鍵暗号化アルゴリズムは、NTRU暗号方式によるものであり、前記公開鍵取得部は、前記公開鍵として、NTRU暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記公開鍵暗号化部は、前記検証値から検証値多項式を生成し、前記ブラインド値からブラインド値多項式を生成し、NTRU暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第1暗号化

情報を生成する。

また、前記公開鍵暗号化アルゴリズムは、NTRU暗号方式によるものであり、前記公開鍵取得部は、前記公開鍵として、NTRU暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記公開鍵暗号化部は、前記検証値から検証値多項式を生成し、ブラインド値を生成し、生成した前記ブラインド値からブラインド値多項式を生成し、NTRU暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第1暗号化情報を生成する。

この構成によると、NTRU暗号を採用することができる。

ここで、前記第2暗号化手段は、前記検証値に一方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第2暗号化情報を生成する。

この構成によると、前記検証値に一方向性関数を施して得られた関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第2暗号化情報を生成するので、不正な第三者は、少なくとも、前記一方向性関数及び前記暗号化アルゴリズムを知っていなければ、前記第2暗号化情報から前記シード値を得ることはできない。

ここで、前記第2暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第2暗号化情報を生成する。

この構成によると、前記暗号化アルゴリズムは、排他的論理和であるので、演算が容易である。また、逆演算が可能である。

ここで、前記第2暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして共通鍵暗号化アルゴリズムを施すことにより、前記第2暗号化情報を生成する。

この構成によると、前記暗号化アルゴリズムは、共通鍵暗号化アルゴリズムであるので、よく知られており、適用が容易である。また、逆演算が可能である。

ここで、前記第2暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして加算を施すことにより、前記第2暗号化情報を生成する。

この構成によると、前記暗号化アルゴリズムは、加算であるので、演算が容易である。また、逆演算が可能である。

ここで、前記第2暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして乗算を施すことにより、前記第2暗号化情報を生成する。

この構成によると、前記暗号化アルゴリズムは、乗算であるので、演算が容易である。また、逆演算が可能である。

ここで、前記第2暗号化手段は、前記検証値に、前記一方向性関数としてハッシュ関数を

施して前記関数値を生成する。

この構成によると、前記一方向性関数は、ハッシュ関数であるので、その演算アルゴリズムがよく知られており、適用が容易である。

ここで、前記第2暗号化手段は、前記検証値を用いて、前記シード値に暗号化アルゴリズムを施して第2暗号化情報を生成する。

この構成によると、前記検証値を用いて、前記シード値に暗号化アルゴリズムを施すので、演算が単純であり、適用が容易である。

ここで、前記第2暗号化手段は、前記検証値及び前記第1暗号化情報を用いて、前記シード値を暗号化する。

この構成によると、前記検証値及び前記第1暗号化情報を用いて、前記シード値を暗号化するので、不正な第三者は、前記検証値及び前記第1暗号化情報を知らなければ、シード値を得ることができず、安全性が高まる。

ここで、前記第2暗号化手段は、前記検証値及び前記第1暗号化情報に一方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第2暗号化情報を生成する。

この構成によると、一方向性関数と暗号化アルゴリズムとを用いるので、不正な第三者は、第1暗号化情報及び第2暗号化情報を知っていても、少なくとも一方向性関数と暗号化アルゴリズムとを知らなければ、シード値を得ることができず、安全性が高まる。

ここで、前記第2暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第2暗号化情報を生成する。

この構成によると、前記暗号化アルゴリズムは、排他的論理和であるので、演算が容易である。また、逆演算が可能である。

ここで、前記共有鍵生成装置は、さらに、コンテンツを取得する取得手段と、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成する暗号化手段とを備え、前記送信手段は、さらに、生成された前記暗号化コンテンツを送信する。

この構成によると、共有鍵生成装置は、第三者に知られることなく、コンテンツを相手の装置へ送信することができる。

ここで、第3者に知られることなく共有鍵生成装置から共有鍵を受け取る共有鍵復元装置であって、前記共有鍵生成装置は、シード値を生成し、生成された前記シード値から検証値及び共有鍵を生成し、生成された前記検証値を暗号化して、第1暗号化情報を生成し、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第2暗号化情報を生成し、生成された前記第1暗号化情報及び前記第2暗号化情報を送信し、前記共有鍵復元装置は、前記第1暗号化情報及び前記第2暗号化情報を受信する受信手段と、受信された前記第1暗号化情報を復号して第1復号検証値を生成する第1復号手段と、生成された前記第1

復号検証値に基づいて、受信された前記第2暗号化情報を復号して、復号シード値を生成する第2復号手段と、前記共有鍵生成装置と同一の方法により、生成された前記復号シード値から第2復号検証値及び復号共有鍵を生成する共有鍵生成手段と、生成された前記第1復号検証値及び前記第2復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断手段と、出力すると判断される場合に、生成された前記復号共有鍵を出力する出力手段とを備える。

この構成によると、共有鍵生成装置から第三者に知られることなく共有鍵を受信できると共に、この際に、共有鍵生成装置と共有鍵復元装置との間で異なる共有鍵が導出されるのを防止できるという効果がある。

ここで、前記共有鍵生成装置は、公開鍵を取得し、取得された前記公開鍵を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第1暗号化情報を生成し、前記第1復号手段は、前記公開鍵に対応する秘密鍵を取得する秘密鍵取得部と、取得された前記秘密鍵を用いて、受信した前記第1暗号化情報に、前記公開鍵暗号化アルゴリズムに対応する公開鍵復号アルゴリズムを施して前記第1復号検証値を生成する公開鍵復号部を含む。

この構成によると、第1復号手段は、公開鍵暗号方式を用いるので、共有鍵暗号方式を用いる場合と比較すると、鍵の管理が容易である。

ここで、前記公開鍵暗号化アルゴリズム及び前記公開鍵復号アルゴリズムは、NTRU暗号方式によるものであり、前記共有鍵生成装置は、前記公開鍵として、NTRU暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記検証値から検証値多項式を生成し、ブラインド値を生成し、生成した前記ブラインド値からブラインド値多項式を生成し、NTRU暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第1暗号化情報を生成し、前記受信手段は、多項式としての前記第1暗号化情報を受信し、前記秘密鍵取得部は、前記秘密鍵として、NTRU暗号方式の鍵生成アルゴリズムにより生成された秘密鍵多項式を取得し、前記公開鍵復号部は、NTRU暗号方式の前記暗号化アルゴリズムに対応する復号アルゴリズムにより、前記秘密鍵多項式を鍵として用いて、多項式としての前記第1暗号化情報を復号して、復号検証値多項式を生成し、生成した前記復号検証値多項式から前記第1復号検証値を生成する。

この構成によると、NTRU暗号を採用することができる。

ここで、前記共有鍵生成装置は、前記検証値に一方方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第2暗号化情報を生成し、前記第2復号手段は、生成された前記第1復号検証値に、前記一方方向性関数を施して復号関数値を生成し、生成した前記復号関数値を用いて、受信された前記第2暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して前記復号シード値を

生成する。

この構成によると、第2復号手段は、一方向性関数及び復号アルゴリズムの2段階による演算方法を採用しているため、不正な第三者は、第1暗号化情報及び第2暗号化情報を知っていても、少なくとも一方向性関数と復号アルゴリズムとを知らなければ、シード値を得ることができず、安全性が高まる。

ここで、前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第2暗号化情報を生成し、前記第2復号手段は、生成した前記復号関数値と前記第2暗号化情報とに、前記復号アルゴリズムとして排他的論理和を施すことにより、前記復号シード値を生成する。

この構成によると、前記復号アルゴリズムは、排他的論理和であるため、演算が容易である。また、前記暗号化アルゴリズムの逆演算である。

ここで、前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして共通鍵暗号化アルゴリズムを施すことにより、前記第2暗号化情報を生成し、前記第2復号手段は、生成した前記復号関数値と前記第2暗号化情報とに、前記復号アルゴリズムとして、前記共通鍵暗号化アルゴリズムに対応する共通鍵復号アルゴリズムを施すことにより、前記復号シード値を生成する。

この構成によると、前記復号アルゴリズムは、共有鍵復号アルゴリズムであるため、よく知られており、適用が容易である。また、前記暗号化アルゴリズムの逆演算である。

ここで、前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして加算を施すことにより、前記第2暗号化情報を生成し、前記第2復号手段は、生成した前記復号関数値と前記第2暗号化情報とに、前記復号アルゴリズムとして、減算を施すことにより、前記復号シード値を生成する。

この構成によると、前記復号アルゴリズムは、減算であるため、演算が容易である。また、前記暗号化アルゴリズムの逆演算である。

ここで、前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして乗算を施すことにより、前記第2暗号化情報を生成し、前記第2復号手段は、生成した前記復号関数値と前記第2暗号化情報とに、前記復号アルゴリズムとして、除算を施すことにより、前記復号シード値を生成する。

この構成によると、前記復号アルゴリズムは、除算であるため、演算が容易である。また、前記暗号化アルゴリズムの逆演算である。

ここで、前記共有鍵生成装置は、前記検証値に、前記一方向性関数としてハッシュ関数を施して前記関数値を生成し、前記第2復号手段は、生成された前記第1復号検証値に、前記一方向性関数として前記ハッシュ関数を施して前記復号関数値を生成する。

この構成によると、前記一方向性関数は、ハッシュ関数であるため、その演算アルゴリズム

ムがよく知られており、適用が容易である。

ここで、前記共有鍵生成装置は、前記検証値を用いて、前記シード値に暗号化アルゴリズムを施して第2暗号化情報を生成し、前記第2復号手段は、生成された前記第1復号検証値を用いて、前記第2暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して、前記復号シード値を生成する。

この構成によると、第1復号検証値を用いて、第2暗号化情報を復号するので、演算が容易である。

ここで、前記共有鍵生成装置は、前記検証値及び前記第1暗号化情報を用いて、前記シード値を暗号化し、前記第2復号手段は、生成された前記第1復号検証値及び受信された前記第1暗号化情報を用いて、前記第2暗号化情報を復号して前記復号シード値を生成する。

この構成によると、第1復号検証値及び第1暗号化情報を用いて、第2暗号化情報を復号するので、不正な第三者は、前記第1復号検証値及び前記第1暗号化情報を知らなければ、シード値を得ることができず、安全性が高まる。

ここで、前記共有鍵生成装置は、前記検証値及び前記第1暗号化情報に一方方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第2暗号化情報を生成し、前記第2復号手段は、前記第1復号検証値及び前記第1暗号化情報に前記一方方向性関数を施して復号関数値を生成し、生成した前記復号関数値を用いて、前記第2暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して、前記復号シード値を生成する。

この構成によると、第2復号手段は、一方方向性関数及び復号アルゴリズムの2段階による演算方法を採用しているので、不正な第三者は、第1暗号化情報及び第2暗号化情報を知っていても、少なくとも一方方向性関数と復号アルゴリズムとを知らなければ、シード値を得ることができず、安全性が高まる。

ここで、前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第2暗号化情報を生成し、前記第2復号手段は、前記復号関数値及び前記第2暗号化情報に、前記復号アルゴリズムとして、排他的論理和を施すことにより、前記復号シード値を生成する。

この構成によると、前記復号アルゴリズムは、排他的論理和であるので、演算が容易である。また、前記暗号化アルゴリズムの逆演算である。

ここで、前記共有鍵生成装置は、前記シード値に一方方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値及び前記共有鍵を生成し、前記共有鍵生成手段は、生成された前記復号シード値に、前記一方方向性関数を施して復号関数値を生成し、生成した前記復号関数値から前記第2復号検証値及び前記復号共有鍵を生成する。

この構成によると、前記復号シード値に一方方向性関数を施して、前記第2復号検証値を生

成するので、前記第2復号検証値を第三者が知り得たとしても、前記第2復号検証値から前記シード値を求めることは困難である。このため、前記第2復号検証値からシード値を求め、さらに、共有鍵を求めることは事実上不可能である。

ここで、前記共有鍵生成装置は、前記シード値に、前記一方向性関数として、ハッシュ関数を施して前記関数値を生成し、前記共有鍵生成手段は、生成された前記復号シード値に、前記一方向性関数として、前記ハッシュ関数を施して前記復号関数値を生成する。

この構成によると、前記一方向性関数は、ハッシュ関数であるので、その演算アルゴリズムがよく知られており、適用が容易である。

ここで、前記共有鍵生成装置は、生成された前記関数値の一部を前記検証値とし、他の一部を前記共有鍵とすることにより、前記検証値及び前記共有鍵を生成し、前記共有鍵生成手段は、生成された前記復号関数値の一部を前記第2復号検証値とし、他の一部を前記復号共有鍵とすることにより、前記第2復号検証値及び前記復号共有鍵を生成する。

この構成によると、前記復号関数値の一部を前記第2復号検証値とし、他の一部を前記復号共有鍵とするので、前記第2復号検証値及び前記復号共有鍵の生成が容易である。

ここで、前記共有鍵生成装置は、前記シード値に一方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値、前記共有鍵及びブラインド値を生成し、公開鍵を取得し、取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第1暗号化情報を生成し、前記共有鍵生成手段は、生成された前記復号シード値に、前記一方向性関数を施して復号関数値を生成し、生成した前記復号関数値から前記第2復号検証値、前記復号共有鍵及び復号ブラインド値を生成する。

この構成によると、前記復号シード値に一方向性関数を施して、前記第2復号検証値を生成するので、前記第2復号検証値を第三者が知り得たとしても、前記第2復号検証値から前記シード値を求めることは困難である。このため、前記第2復号検証値からシード値を求め、さらに、共有鍵を求めることは事実上不可能である。

ここで、前記共有鍵生成装置は、公開鍵を取得し、取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第1暗号化情報を生成し、前記判断手段は、前記第1復号検証値及び前記第2復号検証値に基づく前記判断に代えて、前記公開鍵を取得する公開鍵取得部と、取得された前記公開鍵及び生成された前記復号ブラインド値を用いて、生成された前記第1復号検証値又は前記第2復号検証値に前記公開鍵暗号化アルゴリズムを施して再暗号化情報を生成する再暗号化部と、受信された前記第1暗号化情報及び生成された前記再暗号化情報に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断部とを備える。

この構成によると、受信された前記第1暗号化情報及び生成された前記再暗号化情報に基づいて、生成された前記復号共有鍵を出力するか否かを判断するので、共有鍵生成装置から

第三者に知られることなく共有鍵を受信できると共に、この際に、共有鍵生成装置と共有鍵復元装置との間で異なる共有鍵が導出されるのを防止できるという効果がある。

ここで、前記判断部は、前記第1暗号化情報と前記再暗号化情報とを比較し、前記第1暗号化情報と前記再暗号化情報とが一致する場合に、前記復号共有鍵を出力すると判断する。また、前記判断手段は、前記第1復号検証値と前記第2復号検証値とを比較し、一致する場合に、前記復号共有鍵を出力すると判断する。

この構成によると、第1暗号化情報と再暗号化情報とが一致する場合に、復号共有鍵を出力するので、復号共有鍵を出力するか否かの判断が確実に行える。

ここで、前記公開鍵暗号化アルゴリズムは、NTRU暗号方式によるものであり、前記共有鍵生成装置は、前記公開鍵として、NTRU暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記検証値から検証値多項式を生成し、前記ブラインド値からブラインド値多項式を生成し、NTRU暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第1暗号化情報を生成し、前記公開鍵取得部は、前記公開鍵多項式を取得し、前記再暗号化部は、前記第2復号検証値から復号検証値多項式を生成し、前記復号ブラインド値から復号ブラインド値多項式を生成し、NTRU暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記復号検証値多項式を攪乱するために前記復号ブラインド値多項式を用いて、前記復号検証値多項式を暗号化して、多項式としての前記再暗号化情報を生成する。

この構成によると、NTRU暗号を採用することができる。

ここで、前記共有鍵生成装置は、さらに、コンテンツを取得し、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成し、生成された前記暗号化コンテンツを送信し、前記受信手段は、さらに、前記暗号化コンテンツを受信し、前記共有鍵復元装置は、さらに、出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成する復号手段と、生成された復号コンテンツを出力する出力手段とを備える。

この構成によると、共有鍵生成装置は、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成し、前記共有鍵復元装置は、出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成するので、第三者に知られることなく、共有鍵生成装置から共有鍵復元装置へコンテンツを送信することができるという効果がある。

【BRIEF DESCRIPTION OF THE DRAWINGS】

These and the other objects, advantages and features of

the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings which illustrate a specific embodiment of the invention.

In the drawings:

図1は、コンテンツ配信システム10の構成と、構成要素の間の接続形態とを示す概念図である。

図2は、暗号装置110の構成を示すブロック図である。

図3は、復号装置120の構成を示すブロック図である。

図4は、暗号装置110及び復号装置120の動作を示す処理系統図である。

図5は、暗号装置110及び復号装置120の動作を示すフローチャートである。

図6は、暗号装置110bの構成を示すブロック図である。

図7は、復号装置120bの構成を示すブロック図である。

図8は、暗号装置110b及び復号装置120bの動作を示す処理系統図である。

図9は、暗号装置110cの構成を示すブロック図である。

図10は、復号装置120cの構成を示すブロック図である。

図11は、暗号装置110c及び復号装置120cの動作を示す処理系統図である。

図12は、暗号装置110c及び復号装置120cの変形例の動作を示す処理系統図である。

図13は、暗号装置110dの構成を示すブロック図である。

図14は、復号装置120dの構成を示すブロック図である。

図15は、暗号装置110d及び復号装置120dの動作を示すフローチャートである。

図16は、暗号装置110d及び復号装置120dの動作を示す処理系統図である。

図17は、暗号装置110eの構成を示すブロック図である。

図18は、復号装置120eの構成を示すブロック図である。

図19は、暗号装置110e及び復号装置120eの動作を示す処理系統図である。

図20は、暗号装置110e及び復号装置120eの変形例の動作を示す処理系統図である。

【DESCRIPTION OF THE PREFERRED EMBODIMENT】

1. 実施の形態1

本発明に係る1個の実施の形態としてのコンテンツ配信システム10について説明する。コンテンツ配信システム10は、NTRU暗号を用いて鍵カプセル化メカニズムによる鍵配送を行って暗号化通信を行う暗号通信システムである。

1. 1 NTRU暗号方式

コンテンツ配信システム10において用いるNTRU暗号方式について簡単に説明する。
NTRU暗号方式は、多項式の演算を用いて暗号化と復号化とを行う公開鍵暗号方式である。

なお、NTRU暗号方式及びNTRU暗号方式における公開鍵と秘密鍵との生成方法については、非特許文献2に詳しく述べられている。

(1) NTRU暗号方式のシステムパラメータ

NTRU暗号方式においては、整数のシステムパラメータ、 N 、 p 、 q が存在し、後述する暗号装置及び復号装置は、これらのシステムパラメータを有している。

上記文献には、システムパラメータの例として、 $(N, p, q) = (107, 3, 64)$ 、 $(N, p, q) = (167, 3, 128)$ 、 $(N, p, q) = (503, 3, 256)$ の3つの例が挙げられている。

以降、本実施の形態では、システムパラメータ $N=167$ として、説明を行う。

(2) NTRU暗号方式の多項式演算

NTRU暗号方式は、上述したように、多項式の演算により暗号化と復号化を行う公開鍵暗号方式である。

NTRU暗号方式で扱う多項式は、上記システムパラメータ N に対し、 $N-1$ 次元以下の多項式である。例えば、 $N=5$ のとき、 $X^4 + X^3 + 1$ 等の多項式である。ここで、「 X^a 」は X の a 乗を意味することとする。

また、暗号化時又は復号化時に用いる公開鍵 h 、秘密鍵 f 、平文 m 、乱数 r 、暗号文 c はいずれも、 $N-1$ 次元以下の多項式として表現される（以降、それぞれを公開鍵多項式 h 、秘密鍵多項式 f 、平文多項式 m 、乱数多項式 r 、暗号文多項式 c と呼ぶ）。

多項式演算において、上記システムパラメータ N に対し、関係式 $X^N = 1$ を用いて、演算結果が常に $N-1$ 次元以下の多項式になるように演算される。

例えば、 $N=5$ の場合、多項式 $X^4 + X^2 + 1$ と多項式 $X^3 + X$ の積は、多項式と多項式の積を \times 、整数と多項式の積を \cdot とすると、 $X^5 = 1$ という関係から、

$$\begin{aligned} & (X^4 + X^2 + 1) \times (X^3 + X) \\ &= X^7 + 2 \cdot X^5 + 2 \cdot X^3 + X \\ &= X^2 \times 1 + 2 \cdot 1 + 2 \cdot X^3 + X \\ &= 2 \cdot X^3 + X^2 + X + 2 \end{aligned}$$

となる。

このように、多項式演算において、常に $N-1$ 次元以下の多項式になるように演算される。

(3) NTRU暗号方式の暗号化

後述する暗号装置は、次に示すようにNTRU暗号方式の暗号化を行う。

暗号化時には、以下に述べる乱数多項式 r と公開鍵多項式 h とを用いて、平文多項式 m に多項式演算である暗号化アルゴリズム E を施して、

暗号文多項式 $c = E(m, r, h)$ を生成する。

ここで、 $E(m, r, h)$ は、NTRU暗号方式の暗号化アルゴリズム E に、平文多項式 m 、乱数多項式 r 及び公開鍵多項式 h を入力して得られる多項式演算の結果である。暗号化アルゴリズム E については非特許文献2に詳しく述べられており、ここでは説明を省略する。

なお、NTRU暗号方式では、乱数多項式 r を生成するためのパラメータ d が予め決められている。乱数多項式 r は、乱数多項式 r を構成する各項のうち、 d 個の項についてはその係数が「1」となり、他の d 個の項については係数が「-1」となり、残りの項については係数は「0」となるように、選ばれる。

すなわち、乱数多項式 r は、 $N-1$ 次元以下の多項式であり、0次元（定数項）から $N-1$ 次元までの N 項について、 N 個の係数が存在する。乱数多項式 r は、この N 個の係数のうち、 d 個の係数が「1」であり、かつ d 個の係数が「-1」であり、かつ $(N-2d)$ 個の係数は「0」となるように、選ばれる。

非特許文献2によれば、パラメータ $N=167$ の場合、 $d=18$ である。すなわち、18個の係数が「1」であり、かつ18個の係数が「-1」であり、 $131 (=167-36)$ 個の係数が「0」となるように、乱数多項式 r が選ばれる。

(4) NTRU暗号方式の復号化

後述する復号装置は、次に示すようにNTRU暗号方式の復号化を行う。

復号化時には、秘密鍵多項式 f を用いて、暗号文多項式 c に多項式演算である復号アルゴリズム D を施して、復号文多項式 $m' = D(c, f)$ を生成する。

ここで、 $D(c, f)$ は、NTRU暗号方式の復号アルゴリズム D に、暗号文多項式 c 、及び秘密鍵多項式 f を入力して得られる多項式演算の結果である。復号アルゴリズム D については非特許文献2に詳しく述べられており、ここでは説明を省略する。

(5) NTRU暗号方式の復号エラー

ところで、このNTRU暗号方式において、生成された復号文多項式 m' が平文多項式 m と異なる場合が発生する。この場合は、復号時に正しく平文多項式 m が得られないことになる。このことを復号エラーが発生するという。

1. 2 コンテンツ配信システム10の構成

コンテンツ配信システム10は、図1に示すように、コンテンツサーバ装置140と暗号装置110と復号装置120と再生装置150とモニタ155とから構成されており、コンテンツサーバ装置140と暗号装置110とは、専用回線20を介して接続されており、暗号装置110と復号装置120とは、インターネット130を介して接続されている。再生装置150は、復号装置120及びスピーカを内蔵するモニタ155に接続されている。暗号装置110には、メモリカード160が装着され、復号装置120には、メモリカード170が装着される。

コンテンツサーバ装置140は、映像と音声から構成される映画などのコンテンツを専用回線20を介して暗号装置110へ送信する。

暗号装置110と復号装置120とは、それぞれ同一の共有鍵 K 及び共有鍵 K' を生成する。次に、暗号装置110は、コンテンツサーバ装置140から受け取ったコンテンツを共有鍵 K を用いて暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツを送信し、復号装置120は、暗号化コンテンツを受信し、受信した暗号化コンテンツを復号して再生コンテンツを生成し、再生装置150は、再生コンテンツから映像信号及び音声信号を生成し、モニタ155は、映像を表示し、音声を出力する。

1. 3 コンテンツサーバ装置140の構成

コンテンツサーバ装置140は、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、通信ユニット、キーボード、マウスなどから構成されるコンピュータシステムである（図示していない）。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、コンテンツサーバ装置140は、その一部の機能を達成する。

コンテンツサーバ装置140は、前記コンテンツを予め記憶しており、前記コンテンツは、複数の部分コンテンツ m_i ($1 \leq i \leq n$) から構成されている。コンテンツサーバ装置140は、暗号装置110の要求に応じて、部分コンテンツ m_i を読み出し、読み出した部分コンテンツ m_i を、専用回線20を介して暗号装置110へ送信する。

1. 4 メモリカード160及びメモリカード170の構成

メモリカード160は、記憶媒体としてフラッシュメモリを採用しているカード型の記憶装置であり、予め公開鍵多項式 h を記憶している。

また、メモリカード170は、メモリカード160と同様のカード型の記憶装置であり、予め秘密鍵多項式 f 及び公開鍵多項式 h を記憶している。

ここで、秘密鍵多項式 f と公開鍵多項式 h とは、NTRU暗号方式により生成されたものであり、それぞれ対応している。

1. 5 暗号装置110の構成

暗号装置110は、図2に示すように、公開鍵入力部111、乱数生成部112、第1関数部113、暗号化部114、第1送信部117、共通鍵暗号部118及び第2送信部119から構成されている。

暗号装置110は、具体的には、マイクロプロセッサ、ROM、RAM、通信ユニットなどから構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作

することにより、暗号装置 110 は、その機能を達成する。

(1) 公開鍵入力部 111

公開鍵入力部 111 は、メモリカード 160 から復号装置 120 の公開鍵多項式 h を読み出し、読み出した公開鍵多項式 h を暗号化部 114 へ出力する。

(2) 乱数生成部 112

乱数生成部 112 は、共有鍵 K を生成するための元となるシード値として、乱数 s を生成し、生成した乱数 s を第 1 関数部 113 と暗号化部 114 とへ出力する。

(3) 第 1 関数部 113

第 1 関数部 113 は、乱数生成部 112 から乱数 s を受け取り、乱数 s の関数値 $G(s)$ を生成する。ここで、関数 G は、出力長が $2k$ ビットのハッシュ関数である。なお、ハッシュ関数は、一方向性関数の一種である。次に、第 1 関数部 113 は、関数値 $G(s)$ の上位 k ビットを乱数値 u とし、 $G(s)$ の下位 k ビットを共有鍵 K とすることにより、生成した関数値 $G(s)$ から共有鍵 K と乱数値 u とを生成し、生成した乱数値 u を暗号化部 114 へ出力し、生成した共有鍵 K を共通鍵暗号部 118 へ出力する。

(4) 暗号化部 114

暗号化部 114 は、公開鍵入力部 111 から公開鍵多項式 h を受け取り、乱数生成部 112 から乱数 s を受け取り、第 1 関数部 113 から乱数値 u を受け取る。次に、以下のようにして、NTRU 暗号により、公開鍵多項式 h と乱数値 u とを用いて乱数 s の第 1 暗号文 c_1 を生成する。ここで、乱数値 u は、ブラインド値であり、暗号化の対象である乱数 s を不明瞭にするために用いられる。

暗号化部 114 は、NTRU 暗号のパラメータ d に対し、乱数多項式 r の d 個の項の係数が「1」であり、 d 個の項の係数が「-1」であり、残りの項の係数が「0」である乱数多項式 r を乱数値 u から一意に求まるように生成する。

例えば、暗号化部 114 は、乱数値 u を擬似乱数系列の初期値（乱数シード）として設定し、 $\{0, 1, \dots, N-1\}$ から重複しないように $2d$ 個の擬似乱数を生成し、最初の d 個の擬似乱数によりそれぞれ示される d 個の次元の項の係数を「1」とし、残りの d 個の擬似乱数によりそれぞれ示される d 個の次元の項の係数を「-1」とし、他の次元の項の係数は「0」とする。

次に、暗号化部 114 は、乱数 s が NTRU 暗号の暗号アルゴリズム E に適用できるように、乱数 s を 2 進数表現した場合の N 桁のビット列の各桁の値が、乱数多項式 s_p の各項の係数に対応するように、乱数多項式 s_p を構成する。例えば、乱数 s の下位 b ビット目の値を、項 X^b の係数とする。具体的には、 $s = 10010$ （ビット表現）の場合、乱数多項式 $s_p = X^5 + X^2$ を生成する。

次に、暗号化部 114 は、公開鍵多項式 h を使用して、乱数多項式 r を用いて乱数多項式

s pに前記暗号アルゴリズムEを施して、

第1暗号文c 1＝暗号文多項式E (s p, r, h)を生成する。

次に、暗号化部1 1 4は、生成した第1暗号文c 1を第1送信部1 1 7へ出力する。

なお、図2において、暗号装置1 1 0の各構成部を示す各ブロックは、接続線により他のブロックと接続されている。ここで、各接続線は、信号や情報が伝達される経路を示している。また、暗号化部1 1 4を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが付されているものは、暗号化部1 1 4へ鍵としての情報が伝達される経路を示している。共通鍵暗号部1 1 8を示すブロックについても同様である。また、他の図面についても同様である。

(5) 第1送信部1 1 7

第1送信部1 1 7は、暗号化部1 1 4から第1暗号文c 1を受け取り、第1暗号文c 1をインターネット1 3 0を介して復号装置1 2 0へ送信する。

(6) 共通鍵暗号部1 1 8

共通鍵暗号部1 1 8は、例えばDES暗号方式のような共通鍵暗号アルゴリズムSymを有している。

一般的に、共通鍵暗号では、暗号側の装置において、暗号鍵Kを用いて、平文mに共通鍵暗号アルゴリズムSymを施して、暗号文 $c = \text{Sym}(m, K)$ を生成し、復号側の装置において、暗号鍵Kを用いて、暗号文cに共通鍵暗号アルゴリズムSymを施して、復号文 $m' = \text{Sym}(c, K)$ を生成する。ここで、暗号文生成時に用いる暗号鍵Kと復号文生成時に用いる暗号鍵Kが同一であれば、 $m' = m$ となる。なお、共通鍵暗号及びDES暗号方式については、非特許文献1に詳しく述べられているため、ここでの詳細な説明は省略する。

共通鍵暗号部1 1 8は、コンテンツサーバ装置1 4 0から複数の平文(部分コンテンツ) m_i ($1 \leq i \leq n$)を受け取り、第1関数部1 1 3から共有鍵Kを受け取り、受け取った共有鍵Kを使用して平文 m_i ($1 \leq i \leq n$)に共通鍵暗号アルゴリズムSymを施して、共通鍵暗号文 $C_i = \text{Sym}(m_i, K)$ ($1 \leq i \leq n$)を生成する。

次に、共通鍵暗号部1 1 8は、共通鍵暗号文 C_i ($1 \leq i \leq n$)を第2送信部1 1 9へ出力する。

(7) 第2送信部1 1 9

第2送信部1 1 9は、共通鍵暗号部1 1 8から共通鍵暗号文 C_i ($1 \leq i \leq n$)を受け取り、受け取った共通鍵暗号文 C_i ($1 \leq i \leq n$)を、インターネット1 3 0を介して復号装置1 2 0へ送信する。

1. 6 復号装置1 2 0の構成

復号装置1 2 0は、図3に示すように、秘密鍵入力部1 2 1、第1受信部1 2 2、復号化部1 2 3、第2関数部1 2 6、比較部1 2 7、共通鍵復号部1 2 8及び第2受信部1 2 9か

ら構成される。

復号装置120は、暗号装置110と同様のコンピュータシステムである。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、復号装置120は、その機能を達成する。

(1) 秘密鍵入力部121

秘密鍵入力部121は、メモ리카ード170から、復号装置120の秘密鍵多項式 f と公開鍵多項式 h とを読み出し、読み出した秘密鍵多項式 f を復号化部123へ出力し、読み出した公開鍵多項式 h を比較部127へ出力する。

(2) 第1受信部122

第1受信部122は、インターネット130を介して暗号装置110から第1暗号文 c_1 を受け取り、受け取った第1暗号文 c_1 を復号化部123へ出力する。

(3) 復号化部123

復号化部123は、秘密鍵入力部121から秘密鍵多項式 f を受け取り、第1受信部122から第1暗号文 c_1 を受け取り、次に示すようにして、NTRU暗号により、秘密鍵多項式 f を用いて、第1暗号文 c_1 を復号して復号乱数 s' を生成する。

復号化部123は、秘密鍵多項式 f を使用して、第1暗号文 c_1 に前記復号アルゴリズム D を施して、復号乱数多項式 $s_p' = D(c_1, f)$ を生成する。次に、復号乱数多項式 s_p' は、NTRU暗号の復号文であり多項式で表現されているので、復号乱数多項式 s_p' の各項の係数が、復号乱数 s' を2進数表現した場合の N 桁のビット列の各値に対応するように、復号乱数 s' を生成する。例えば、復号乱数多項式 s_p' の b 次元の項 X^b の係数は、復号乱数 s' の下位 b ビット目の値となる。

具体的には、復号乱数多項式 $s_p' = X^5 + X^2$ の場合、復号乱数 $s' = 10010$ (ビット表現)を生成する。

次に、復号化部123は、受け取った第1暗号文 c_1 と生成した復号乱数 s' とを比較部127へ出力し、生成した復号乱数 s' を第2関数部126へ出力する。

(4) 第2関数部126

第2関数部126は、第1関数部113が有している関数と同じ関数 G のアルゴリズムを有している。

第2関数部126は、復号化部123から復号乱数 s' を受け取り、第1関数部113と同様にして、復号乱数 s' の関数値 $G(s')$ を生成し、次に、関数値 $G(s')$ から乱数値 u' と共有鍵 K' とを生成し、生成した乱数値 u' と共有鍵 K' とを比較部127へ出力する。

(5) 比較部127

比較部127は、図3に示すように、暗号化部127xと比較演算部127yとから構成

されている。

暗号化部127xは、秘密鍵入力部121から公開鍵多項式 h を受け取り、復号化部123から復号乱数 s' を受け取り、第2関数部126から乱数値 u' を受け取る。次に、暗号化部114と同様にして、公開鍵多項式 h と乱数値 u' とを用いて、復号乱数 s' を暗号化して第1再暗号文 $c1'$ を生成し、生成した第1再暗号文 $c1'$ を比較演算部127yへ出力する。

比較演算部127yは、復号化部123から第1暗号文 $c1$ を受け取り、第2関数部126から共有鍵 K' を受け取り、暗号化部127xから第1再暗号文 $c1'$ を受け取る。次に、第1暗号文 $c1$ と第1再暗号文 $c1'$ とを比較して、一致しているか否かを判断し、一致していると判断する場合に、受け取った共有鍵 K' を共通鍵復号部128へ出力する。一致しないと判断する場合に、受け取った共有鍵 K' を出力しない。

(6) 第2受信部129

第2受信部129は、インターネット130を介して暗号装置110から共通鍵暗号文 C_i ($1 \leq i \leq n$)を受信し、受信した共通鍵暗号文 C_i ($1 \leq i \leq n$)を共通鍵復号部128へ出力する。

(7) 共通鍵復号部128

共通鍵復号部128は、共通鍵暗号部118が有する共通鍵暗号アルゴリズム Sym と同じ共通鍵暗号アルゴリズム Sym を予め有している。

共通鍵復号部128は、比較部127から共有鍵 K' を受け取り、第2受信部129から共通鍵暗号文 C_i ($1 \leq i \leq n$)を受け取り、受け取った共有鍵 K' を使用して受け取った共通鍵暗号文 C_i ($1 \leq i \leq n$)に共通鍵暗号アルゴリズム Sym を施して、復号文 $m_i' = Sym(C_i, K)$ ($1 \leq i \leq n$)を生成する。

次に、共通鍵復号部128は、生成した復号文 m_i' ($1 \leq i \leq n$)を再生装置150へ出力する。

1. 7 再生装置150及びモニタ155

再生装置150は、復号装置120から復号文 m_i' ($1 \leq i \leq n$)を受け取り、受け取った復号文 m_i' ($1 \leq i \leq n$)から映像信号及び音声信号を生成し、生成した映像信号及び音声信号をモニタ155へ出力する。

モニタ155は、再生装置150から映像信号及び音声信号を受け取り、受け取った映像信号及び音声信号により、映像を表示し、音声を出力する。

1. 8 暗号装置110及び復号装置120の動作

暗号装置110及び復号装置120の動作について、図4に示す処理系統図及び図5に示すフローチャートを用いて説明する。

暗号装置110の公開鍵入力部111は、メモリカード160から復号装置120の公開

鍵多項式 h を読み出し、読み出した公開鍵多項式 h を暗号化部114へ出力する（ステップS101）。

次に、乱数生成部112は、乱数 s を生成し、生成した乱数 s を第1関数部113と暗号化部114とへ出力する（ステップS102）。

次に、第1関数部113は、乱数生成部112から乱数 s を受け取り、乱数 s の関数値 $G(s)$ を生成し（ステップS103）、次に、第1関数部113は、関数値 $G(s)$ から乱数値 u と共有鍵 K とを生成して、乱数値 u を暗号化部114へ出力し、共有鍵 K を共通鍵暗号部118へ出力する（ステップS104）。

次に、暗号化部114は、公開鍵入力部111から公開鍵多項式 h を受け取り、乱数生成部112から乱数 s を受け取り、第1関数部113から乱数値 u を受け取り、公開鍵多項式 h と乱数値 u を用いて乱数 s の第1暗号文 c_1 を生成し、第1暗号文 c_1 を第1送信部117へ出力する（ステップS105）。

次に、第1送信部117は、暗号化部114から第1暗号文 c_1 を受け取り、第1暗号文 c_1 をインターネット130を介して復号装置120へ送信する（ステップS106）。

次に、復号装置120の秘密鍵入力部121は、メモリカード170から復号装置120の秘密鍵多項式 f と公開鍵多項式 h とを読み出し、読み出した秘密鍵多項式 f を復号化部123へ出力し、読み出した公開鍵多項式 h を比較部127へ出力する（ステップS151）。

次に、第1受信部122は、インターネット130を介して暗号装置110から第1暗号文 c_1 を受け取り、第1暗号文 c_1 を復号化部123へ出力する（ステップS106）。

次に、復号化部123は、秘密鍵入力部121から秘密鍵多項式 f を受け取り、第1受信部122から第1暗号文 c_1 を受け取り、次に、秘密鍵多項式 f を用いて、第1暗号文 c_1 を復号して復号乱数 s' を生成し、第1暗号文 c_1 と復号乱数 s' を比較部127へ出力し、復号乱数 s' を第2関数部126へ出力する（ステップS152）。

次に、第2関数部126は、復号化部123から復号乱数 s' を受け取り、復号乱数 s' の関数値 $G(s')$ を生成し（ステップS153）、関数値 $G(s')$ から乱数値 u' と共有鍵 K' とを生成して、乱数値 u' と共有鍵 K' とを比較部127へ出力する（ステップS154）。

次に、比較部127は、復号化部123から第1暗号文 c_1 を受け取り、第2関数部126から乱数値 u' と共有鍵 K' とを受け取り、第1再暗号文 c_1' を生成し（ステップS155）、第1暗号文 c_1 が乱数値 u' を用いた復号乱数 s' の暗号文であるかどうかチェックを行い、第1暗号文 c_1 が復号乱数 s' の暗号文でなければ（ステップS156）、復号装置120は、処理を終了する。

共通鍵暗号部118は、外部から複数の平文 m_i ($1 \leq i \leq n$)を受け取り、第1関数部113から共有鍵 K を受け取り、共有鍵 K を使用して平文 m_i ($1 \leq i \leq n$)に共通鍵暗号

アルゴリズム Sym を施して、共通鍵暗号文 $C_i = Sym(m_i, K)$ ($1 \leq i \leq n$) を生成し、共通鍵暗号文 C_i ($1 \leq i \leq n$) を第2送信部119へ出力する(ステップS107)。

次に、第2送信部119は、共通鍵暗号部118から共通鍵暗号文 C_i ($1 \leq i \leq n$) を受け取り、インターネット130を介して復号装置120へ送信し(ステップS108)、処理を終了する。

第1暗号文 c_1 が復号乱数 s' の暗号文であれば(ステップS156)、比較部127は、共有鍵 K' を共通鍵復号部128へ出力する(ステップS157)。次に、第2受信部129は、インターネット130を介して暗号装置110から暗号文 C_i ($1 \leq i \leq n$) を受信し、共通鍵復号部128へ出力する(ステップS108)。

次に、共通鍵復号部128は、比較部127から共有鍵 K' を受け取り、第2受信部129から共通鍵暗号文 C_i ($1 \leq i \leq n$) を受け取り、共有鍵 K' を使用して共通鍵暗号文 C_i ($1 \leq i \leq n$) に共通鍵暗号アルゴリズム Sym を施して、復号文 $m_i' = Sym(C_i, K)$ ($1 \leq i \leq n$) を生成し、復号文 m_i' ($1 \leq i \leq n$) を再生装置150へ出力し(ステップS158)、処理を終了する。

1. 9 コンテンツ配信システム10の動作検証

以下に、実施の形態1におけるコンテンツ配信システム10の全体の動作について説明する。

まず、暗号装置110は、復号装置120の公開鍵多項式 h を入力とし、乱数 s を生成し、関数値 $G(s)$ から乱数値 u と共有鍵 K とを導出する。次に、暗号装置110は、乱数 s を、公開鍵多項式 h と乱数値 u を用いてNTRU暗号で暗号化して第1暗号文 c_1 を生成し、第1暗号文 c_1 をインターネット130を介して復号装置120へ送信する。

すなわち、この暗号装置110は、以下の処理を行い、第1暗号文 c_1 を復号装置120へ送信する。

- ・乱数 s を生成する。
- ・ $G(s)$ を生成し、 $G(s)$ から u 、 K を生成する。
- ・公開鍵多項式 h と乱数値 u とを用いて乱数 s の第1暗号文 c_1 を生成する。
- ・共有鍵 K と第1暗号文 c_1 とを出力する。

次に、暗号装置110は、導出した共有鍵 K を用いて、外部から入力された平文 m_i ($1 \leq i \leq n$) を共通鍵暗号で暗号化して暗号文 C_i ($1 \leq i \leq n$) を生成し、インターネット130を介して復号装置120へ送信する。

一方、復号装置120は、復号装置120の秘密鍵多項式 f 及び公開鍵多項式 h を入力とし、インターネット130を介して暗号装置110から第1暗号文 c_1 を受信し、第1暗号文 c_1 を秘密鍵多項式 f を用いて復号して復号乱数 s' を生成する。次に、復号乱数 s' の関数値 $G(s')$ から乱数値 u' と共有鍵 K' を導出し、復号乱数 s' を暗号化して第1再暗

号文 c_1' を生成し、 $c_1' = c_1$ であれば、共有鍵 K' を出力する。

すなわち、この復号装置 120 は、以下の処理を行い、共有鍵 K' を導出する。

- ・秘密鍵多項式 f を用いて第 1 暗号文 c_1 を復号して s' を生成する。
- ・ $G(s')$ を生成し、 $G(s')$ から u' 、 K' を生成する。
- ・公開鍵多項式 h 、乱数値 u' を用いて s' の第 1 再暗号文 c_1' を生成する。
- ・ $c_1' = c_1$ が成立するかどうかチェックする。成立すれば共有鍵 K' を出力する。

ここで、暗号装置 110 で用いられた公開鍵多項式 h に対応する正しい秘密鍵多項式 f が復号装置 120 で用いられれば、第 1 暗号文 c_1 は正しく復号されて、復号乱数 $s' = s$ となり、従って、 $G(s')$ から導出される乱数値 $u' = u$ となり、共有鍵 $K' = K$ となる。そして、 $s' = s$ 及び $u' = u$ が成り立つので、 $c_1' = c_1$ が成り立ち、復号装置 120 は暗号装置 110 と同じ共有鍵 K を導出できることになる。

次に、復号装置 120 は、導出した共有鍵 K' ($=K$) を用いて、インターネットを介して暗号装置 110 から共通鍵暗号文 C_i ($1 \leq i \leq n$) を共通鍵暗号で復号して復号文 m_i' ($1 \leq i \leq n$) を生成して外部へ出力する。ここで、共通鍵暗号文生成時に用いた暗号鍵 K と復号文生成時に用いる暗号鍵 K' とは同一であるで、復号装置 120 は、正しく $m_i' = m_i$ ($1 \leq i \leq n$) を得ることができる。

なお、復号エラーが発生した場合には、復号乱数 s' と乱数 s とは異なるので、 $G(s')$ から導出される乱数値 u' 及び共有鍵 K' は、それぞれ u 、 K とは異なる。しかし、この場合、 s' 、 u' がそれぞれ s 、 u と異なるために第 1 再暗号文 c_1' が第 1 暗号文 c_1 と異なるので、復号装置 120 は、共有鍵 K' を出力しない。

1. 10 実施の形態 1 における効果

従来の RSA-KEM アルゴリズムでは、秘密鍵を知らなければ暗号文 C から導出できない要素 s をハッシュ関数 G に入力して共有鍵 K を導出する。しかしながら、NTRU 暗号を用いて、鍵カプセル化メカニズムである RSA-KEM アルゴリズムを適用して共有鍵の配送を行おうとすると、復号エラーが発生する場合があるため、秘密鍵を用いても要素 s が導出できず、従って正しくない共有鍵 K' を導出する場合がある。

しかしながら、実施の形態 1 のコンテンツ配信システム、暗号装置及び復号装置においては、乱数 s のハッシュ関数値 $G(s)$ から共有鍵に加えて乱数値 u を生成し、復号装置が乱数値 u と公開鍵多項式 h とを用いて復号乱数 s' を再暗号化して第 1 再暗号文 c_1' を生成し、第 1 再暗号文 c_1' が第 1 暗号文 c_1 と同じ値でない限り共有鍵 K' を出力しないようにしたので、復号エラーが発生した場合、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できる。

また、本発明による方式は、非特許文献 3 に記述されている証明方法と同様の方法により、理論的にその安全性が証明できる。

1. 1 1 変形例

上記に説明した実施の形態1は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その主旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

(1) 用いるNTRU暗号のパラメータ $N=167$ に限定されない。パラメータ N は、他の値をとるとしてもよい。

(2) 暗号化部114及び復号化部123で行われるビット列の各ビットの値と多項式の各項の係数との変換方法は、上記において説明した方法に限られず他の変換方法でもよい。

例えば、乱数 s から乱数多項式 s_p への変換は、ビット列の各ビットの値と多項式の各項の係数とを1対1に対応させる関数を用いて変換してもよいし、また、ビット列の各ビットの値と多項式の各項の係数とを1対1に対応させて記憶している関数値テーブルを用いて変換してもよい。

また、乱数値 u から乱数多項式 r への変換は、 u から r が一意に求まり、 r の d 個の次元の項の係数を「1」とし、 d 個の次元の項の係数を「-1」とし、他の次元の項の係数は「0」となるようにすれば、他の変換方法でもよく、例えば、乱数値 u を多項式に対応させる関数、又は関数値テーブルを用いて変換してもよい。

(3) 暗号化部114及び復号化部123で用いる公開鍵暗号方式は、暗号化部114において、乱数 s を公開鍵と乱数値 u を用いて暗号化して第1暗号文 c_1 を生成し、復号化部123において、第1暗号文 c_1 を秘密鍵で復号して乱数値 s と等しい復号乱数 s' を生成できるものであればよい。

従って、暗号化部114及び復号化部123で用いる公開鍵暗号は、NTRU暗号以外に、どんな公開鍵暗号でも利用できる。

例えば、ElGamal暗号を採用するならば、 h 、 f をそれぞれElGamal暗号の公開鍵、秘密鍵とし、暗号化部114において、乱数 s を h と u を用いて暗号化して c_1 を生成し、復号化部123において、 c_1 を f を用いて復号して s' を生成すればよい。

なお、ElGamal暗号について非特許文献1に詳細に記載されているため、ここでは説明を省略する。

(4) 第1関数部113は、関数値 $G(s)$ の上位 k ビットを乱数値 u とし、下位 k ビットを共有鍵 K とする以外に、関数値 $G(s)$ から乱数値 u と共有鍵 K とを導出すれば他の方法でもよい。

例えば、関数値 $G(s)$ の上位 $k/2$ ビットを乱数値 u とし、下位 $k \times 3/2$ ビットを共有鍵 K としてもよい。また、関数値 $G(s)$ の $2k$ ビットのうち、1ビット置きに k ビットを選択して乱数値 u とし、残りの k ビットを共有鍵 K としてもよい。

(5) 乱数値 u は、第1関数部113及び第2関数部126で生成される以外にも、暗号

装置110と復号装置120とで同じ値を得られれば、他の生成方法を採用してもよい。

例えば、任意の関数 $Func$ に対し、 $u = Func(s)$ として暗号装置110と復号装置120とで同じ値を得られるようにしてもよい。すなわち、暗号装置110と復号装置120とにおいて、

- ・ $G(s)$ を生成し、 $G(s)$ から K を生成する。
- ・ $Func(s)$ を生成し、 $u = Func(s)$ とする。

としてもよい。

(6) 乱数値 u は、第1関数部113及び第2関数部126で生成される以外にも、暗号装置110と復号装置120とで同じ値を得られればよいので、暗号装置110が乱数値 u を復号装置120bに直接送信してもよい。

すなわち、以下のように、第1暗号文 c_1 と乱数値 u を復号装置120に送信してもよい。このとき、乱数値 u は暗号化して送信されてもよい。

暗号装置110において、

- ・ $G(s)$ を生成し、 $G(s)$ から K を生成する。
- ・ 乱数値 u を、別途、暗号装置110から復号装置120へ送信する。

復号装置120において、

- ・ 乱数値 u を受信する。
- ・ 乱数値 u' に代えて、受信した乱数値 u を用いて第1再暗号文 c_1' を生成する。

このとき、暗号装置110は、乱数値 u を暗号化して送信し、復号装置120は、暗号化された乱数値 u を復号するとしてもよい。

(7) 乱数値 u は、暗号装置110と復号装置120とで同じ値を得られればよいので、乱数値 u の一部分の部分情報を第1関数部113及び第2関数部126で生成し、乱数値 u の残りの部分の部分情報を暗号装置110から復号装置120に直接送信してもよい。

例えば、以下のように、暗号装置110は、第1暗号文 c_1 と乱数値 u_2 とを復号装置120に送信してもよい。

暗号装置110において、

- (a) $G(s)$ を生成し、 $G(s)$ から K 、 u_1 を生成する。
- (b) 乱数値 u_2 を生成し、別途、復号装置120へ送信する。
- (c) 乱数値 u を、 $u = u_1 \text{ xor } u_2$ から生成する。
- (d) 乱数値 u を用いて、第1暗号文 c_1 を生成する。

復号装置120において、

- (e) 乱数値 u_2 を受信する。
- (f) $G(s')$ を生成し、 $G(s')$ から K' 、 u_1' を生成する。
- (g) 乱数値 u' を、 $u' = u_1' \text{ xor } u_2$ から生成する。

(h) 生成した乱数値 u' を用いて第1再暗号文 $c1'$ を生成する。

このとき、暗号装置110は、乱数値 $u2$ を暗号化して送信し、復号装置120は、暗号化された乱数値 $u2$ を復号するとしてもよい。

また、(c) 及び (g) において、排他的論理和 xor に代えて他の演算を用いるとしてもよい。例えば、(c) 及び (g) において、それぞれ加算及び減算を用いてもよいし、また、乗算及び除算を用いてもよい。

(8) 復号エラーの発生により暗号装置110と復号装置120との間で異なる共有鍵が導出されるのを防止するため、第1再暗号文 $c1'$ と第1暗号文 $c1$ とが同じである場合に、共有鍵 K' を出力する代わりに、暗号装置110が乱数 s 、乱数値 u 、共有鍵 K のいずれか1つ以上について、ハッシュ関数値を生成し、生成したハッシュ関数値を復号装置120へ送信し、復号装置120がこのハッシュ関数値を検証することにより、共有鍵 K' を出力するか否かを決定してもよい。例えば、このハッシュ関数値として、任意のハッシュ関数 H に対して、乱数 s のハッシュ関数値 $H(s)$ を生成するようにしてもよいし、乱数 s 、乱数値 u 、共有鍵 K の組み合わせ、例えば、ハッシュ関数値 $H(s || u || k)$ やハッシュ関数値 $H(u || k)$ 等を生成するようにしてもよい。

また、この場合、暗号装置110の第1関数部113は、関数値 $G(s)$ から乱数値 u と共有鍵 K を導出する代わりに、 $G(s)$ から共有鍵 K のみを導出してもよい。

以下に、その具体例を述べる。

コンテンツ配信システム10は、暗号装置110及び復号装置120に代えて、暗号装置110b及び復号装置120bを含み、暗号装置110bは、図6に示すように、公開鍵入力部111、乱数生成部112、第1関数部113b、暗号化部114b、第1送信部117b、共通鍵暗号部118及び第2送信部119から構成されており、復号装置120は、図7に示すように、秘密鍵入力部121b、第1受信部122b、復号化部123b、第2関数部126b、比較部127b、共通鍵復号部128及び第2受信部129から構成される。比較部127bは、第3関数部127u及び比較演算部127vを含む。

暗号装置110bが乱数 s のハッシュ関数値を生成し、復号装置120bがこのハッシュ関数値を検証する際に、暗号装置110bにおいて、図8の処理系統図に示すように、第1関数部113bは、 $G(s)$ を生成し（ステップS103）、 $G(s)$ から K を生成する（ステップS104）。

次に、暗号化部114bは、乱数値 u を生成し、生成した乱数値 u から乱数多項式 r を生成し、乱数多項式 r 及び公開鍵多項式 h を用いて乱数 s の第1暗号文 $c1$ を生成し（ステップS105）、ハッシュ関数値 $H(s)$ を生成する（ステップS111）。

次に、第1送信部117bは、第1暗号文 $c1$ を送信し（ステップS106）、ハッシュ関数値 $H(s)$ を送信する（ステップS112）。

次に、復号装置120bにおいて、第1受信部122bは、第1暗号文c1を受信し（ステップS106）、ハッシュ関数値H（s）を受信する（ステップS112）。

次に、復号化部123bは、秘密鍵多項式fを用いて第1暗号文c1を復号してs'を生成する（ステップS152）。

次に、第2関数部126は、G（s'）を生成し（ステップS153）、G（s'）からK'を生成する（ステップS154）。

次に、比較部127は、第3関数部127uにより、H（s'）を生成し（ステップS154）、比較演算部127vにより、H（s'）=H（s）が成立するかどうかチェックし（ステップS162）、成立すれば共有鍵K'を出力する（ステップS157）。

また、この場合、さらに安全性を高めるために、特許文献1に開示されている方法を用いて、乱数sに付加情報を附したものを暗号化して第1暗号文c1を生成してもよい。すなわち、図6において、暗号化部114bは、付加情報Raを生成し、sとRaのビット結合s || Raの値を暗号化して第1暗号文c1を生成し、図7において、復号化部123bは、第1暗号文c1を復号してs' || Ra'を生成し、Ra'を除去して復号乱数s'を生成してもよい。

また、特許文献1に開示されている通り、s || Raの値の代わりに、sとRaの可逆変換F（s，Ra）の値を用いてもよい。

2. 実施の形態2

本発明に係る別の実施の形態としてのコンテンツ配信システム10c（図示していない）について説明する。

コンテンツ配信システム10cは、コンテンツ配信システム10を基本としてこれを変形したシステムであり、関数値G（s）から乱数値uと共有鍵Kとの他にさらに検証値aを生成する点と、暗号装置が、乱数sを暗号化した第1暗号文c1を生成して送信する代わりに、検証値aを暗号化した第1暗号文c1と、乱数sを検証値aに基づいて暗号化した第2暗号文c2とを生成して送信する点において、コンテンツ配信システム10と異なる。

以下、コンテンツ配信システム10cについて、上記差異点を中心に詳しく説明する。

2. 1 コンテンツ配信システム10cの構成

コンテンツ配信システム10cは、コンテンツ配信システム10と同様の構成を有しており、暗号装置110及び復号装置120に代えて、暗号装置110c及び復号装置120cを含んでいる。その他の構成については、コンテンツ配信システム10におけるものと同様であるので説明を省略する。

2. 2 暗号装置110cの構成

暗号装置110cは、図9に示すように、暗号装置110と同様の構成を有しており、乱数生成部112、第1関数部113、暗号化部114及び第1送信部117に代えて、乱数

生成部112c、第1関数部113c、暗号化部114c、乱数マスク部116c及び第1送信部117cを含む。

ここでは、乱数生成部112c、第1関数部113c、暗号化部114c、乱数マスク部116c及び第1送信部117cについて説明する。

(1) 乱数生成部112c

乱数生成部112cは、共有鍵Kを生成するための元となるシード値として、乱数sを生成し、生成した乱数sを第1関数部113bと乱数マスク部116cとへ出力する。

(2) 第1関数部113c

第1関数部113cは、乱数生成部112cから乱数sを受け取り、乱数sの関数値 $G(s)$ を生成する。次に、生成した関数値 $G(s)$ から検証値aと共有鍵Kと乱数値uとを生成する。

ここで、関数Gは、出力長が3kビットのハッシュ関数であり、第1関数部113cは、関数値 $G(s)$ の上位kビットを検証値aとし、関数値 $G(s)$ の中間のkビットを共有鍵Kとし、関数値 $G(s)$ の下位kビットを乱数値uとする。

次に、第1関数部113cは、生成した検証値aと乱数値uとを暗号化部114cへ出力し、生成した共有鍵Kを共通鍵暗号部118へ出力し、生成した検証値aを乱数マスク部116cへ出力する。

(3) 暗号化部114c

暗号化部114cは、公開鍵入力部111から公開鍵多項式hを受け取り、第1関数部113cから検証値aと乱数値uとを受け取り、次に示すようにして、公開鍵多項式hと乱数値uとを用いて検証値aの第1暗号文c1を生成する。ここでは、第1暗号文c1はNTRU暗号による暗号文である。

暗号化部114cは、NTRU暗号のパラメータdに対し、d個の項の各係数が「1」であり、他のd個の項の各係数が「-1」であり、残りの項の各係数が「0」となる乱数多項式rを乱数値uから一意に求まるように生成する。具体的には、乱数値uを擬似乱数系列の初期値（乱数シード）として設定し、 $\{0, 1, \dots, N-1\}$ から重複しないように2d個の擬似乱数を選択し、最初のd個の擬似乱数により示される次元の項の係数を「1」とし、他のd個の擬似乱数により示される次元の係数を「-1」とし、残りの項の係数を「0」とすることにより、乱数多項式rを生成する。

次に、受け取った検証値aがNTRU暗号の暗号アルゴリズムEに適用できるように、暗号化部114cは、検証値aを2進数表現した場合におけるN桁のビット列の各桁の値が、検証値多項式 a_p の各項の係数に対応するように、検証値多項式 a_p を構成することにより、検証値aを検証値多項式 a_p に変換する。例えば、検証値aの下位bビット目の値は、項 X^b の係数の値となる。具体的には、検証値 $a = 10010$ （ビット表現）の場合、検証値

多項式 $a_p = X^5 + X^2$ を生成する。

次に、暗号化部114cは、公開鍵多項式 h を鍵として使用して、乱数多項式 r を用いて検証値多項式 a_p に前記暗号アルゴリズム E を施して、暗号文多項式である第1暗号文 $c_1 = E(a_p, r, h)$ を生成する。

次に、暗号化部114cは、生成した第1暗号文 c_1 を第1送信部117cへ出力する。

(4) 乱数マスク部116c

乱数マスク部116cは、乱数生成部112cから乱数 s を受け取り、第1関数部113cから検証値 a を受け取り、次に、第2暗号文 $c_2 = s \text{ xor } a$ を生成し、生成した第2暗号文 c_2 を第1送信部117cへ出力する。

ここで、 xor は排他的論理和演算を表す演算子である。

なお、乱数マスク部116cは、排他的論理和に代えて、共有鍵暗号アルゴリズム、加算又は乗算を用いるとしてもよい。

(5) 第1送信部117c

第1送信部117cは、暗号化部114cから第1暗号文 c_1 を受け取り、乱数マスク部116cから第2暗号文 c_2 を受け取り、受け取った第1暗号文 c_1 と第2暗号文 c_2 とを、インターネット130を介して復号装置120cへ送信する。

2. 2 復号装置120cの構成

復号装置120cは、図10に示すように、復号装置120と同様の構成を有しており、第1受信部122c、復号化部123c、第2関数部126c及び比較部127cに代えて、第1受信部122c、復号化部123c、乱数マスク除去部125c、第2関数部126c及び比較部127cを含む。

ここでは、第1受信部122c、復号化部123c、乱数マスク除去部125c、第2関数部126c及び比較部127cについて説明する。

(1) 第1受信部122c

第1受信部122cは、インターネット130を介して、暗号装置110cから第1暗号文 c_1 と第2暗号文 c_2 とを受け取り、受け取った第1暗号文 c_1 を復号化部123cへ出力し、受け取った第2暗号文 c_2 を乱数マスク除去部125cへ出力する。

(2) 復号化部123c

復号化部123cは、秘密鍵入力部121cから秘密鍵多項式 f を受け取り、第1受信部122cから第1暗号文 c_1 を受け取り、次に示すようにして、秘密鍵多項式 f を用いて、第1暗号文 c_1 を復号して復号検証値 a' を生成する。ここでは、復号検証値 a' はNTRU暗号による復号文である。

復号化部123cは、秘密鍵多項式 f を鍵として使用して、第1暗号文 c_1 に前記復号アルゴリズム D を施して、復号検証値多項式 $a_p' = D(c_1, f)$ を生成する。ここで、復号

検証値多項式 $a p'$ は、NTRU暗号の復号文であり多項式で表現されているので、復号化部123cは、復号検証値多項式 $a p'$ の各項の係数が、2進数表現されたN桁のビット列である復号検証値 a' の各桁の値に対応するように、復号検証値多項式 $a p'$ を復号検証値 a' に変換する。例えば、復号検証値多項式 $a p'$ のb次元の項 X^b の係数を、復号検証値 a' の下位bビット目の値とする。具体的には、復号検証値多項式 $a p' = X^5 + X^2$ の場合、復号検証値 $a' = 10010$ (ビット表現) に変換する。

次に、復号化部123cは、生成した復号検証値 a' を乱数マスク除去部125cへ出力し、受け取った第1暗号文 $c1$ を比較部127cへ出力する。

(3) 乱数マスク除去部125c

乱数マスク除去部125cは、第1受信部122cから第2暗号文 $c2$ を受け取り、復号化部123cから復号検証値 a' を受け取り、復号乱数 $s' = c2 \text{ xor } a'$ を生成し、生成した復号乱数 s' を第2関数部126cへ出力する。

なお、乱数マスク部116cが、排他的論理和に代えて、共有鍵暗号アルゴリズム、加算又は乗算を用いる場合において、乱数マスク除去部125cは、それぞれ、共有鍵暗号アルゴリズムに対応する共有鍵復号アルゴリズム、減算、又は除算を用いるとしてもよい。

(4) 第2関数部126c

第2関数部126cは、第1関数部113cが有する関数と同じ関数Gによるアルゴリズムを有している。

第2関数部126cは、乱数マスク除去部125cから復号乱数 s' を受け取り、受け取った復号乱数 s' の関数値 $G(s')$ を生成する。次に、第1関数部113cと同様にして、関数値 $G(s')$ から検証値 a'' と共有鍵 K' と乱数値 u' とを生成し、生成した検証値 a'' と共有鍵 K' と乱数値 u' とを比較部127cへ出力する。

(5) 比較部127c

比較部127cは、図10に示すように、比較演算部127s及び暗号化部127tから構成されている。

暗号化部127tは、秘密鍵入力部121から公開鍵多項式 h を受け取り、第2関数部126cから検証値 a'' と乱数値 u' とを受け取り、受け取った公開鍵多項式 h と乱数値 u' を用いて、暗号化部114cと同様にして検証値 a'' を暗号化して第1再暗号文 $c1'$ を生成し、生成した第1再暗号文 $c1'$ を比較演算部127sへ出力する。

また、比較演算部127sは、第2関数部126cから共有鍵 K' を受け取り、復号化部123cから第1暗号文 $c1$ を受け取り、暗号化部127tから第1再暗号文 $c1'$ を受け取り、次に、受け取った第1暗号文 $c1$ と、受け取った第1再暗号文 $c1'$ とを比較し、第1暗号文 $c1 = \text{第1再暗号文 } c1'$ であると判断する場合に、受け取った共有鍵 K' を共通

鍵復号部128へ出力する。

2. 3 コンテンツ配信システム10cの動作

以下に、実施の形態2におけるコンテンツ配信システム10cの全体の動作について、図11に示す処理系統図を用いて、説明する。

暗号装置110cは、復号装置120cの公開鍵多項式 h を受け取り(ステップS101)、乱数 s を生成し(ステップS102)、関数値 $G(s)$ を求め、関数値 $G(s)$ から検証値 a 、共有鍵 K 及び乱数値 u を導出する(ステップS121)。次に、暗号装置110cは、検証値 a を、公開鍵多項式 h 及び乱数値 u を用いてNTRU暗号により暗号化して第1暗号文 $c1$ を生成し(ステップS105)、検証値 a に基づき乱数 s を暗号化して第2暗号文 $c2 = s \text{ xor } a$ を生成する(ステップS122)。次に、暗号装置110cは、第1暗号文 $c1$ と第2暗号文 $c2$ とをインターネット130を介して復号装置120cへ送信する(ステップS106)。

すなわち、この暗号装置110cは、以下の処理を行い、暗号文 $C = (c1, c2)$ を復号装置120cへ送信する。

- (a) 乱数 s を生成する。
- (b) $G(s)$ を生成し、 $G(s)$ から a 、 K 、 u を生成する。
- (c) 公開鍵多項式 h 、乱数値 u を用いて検証値 a の第1暗号文 $c1$ を生成する。
- (d) $c2 = s \text{ xor } a$ を生成する。

次に、暗号装置110cは、導出した共有鍵 K を用いて、コンテンツサーバ装置140から受け取った平文 m_i ($1 \leq i \leq n$)を共通鍵暗号方式により暗号化して暗号文 C_i ($1 \leq i \leq n$)を生成し(ステップS107)、インターネット130を介して復号装置120cへ送信する(ステップS108)。

一方、復号装置120cは、復号装置120cの秘密鍵多項式 f 及び公開鍵多項式 h を受け取り(ステップS151)、インターネット130を介して暗号装置110cから第1暗号文 $c1$ と第2暗号文 $c2$ を受信し(ステップS106)、第1暗号文 $c1$ を秘密鍵多項式 f を用いて復号して復号検証値 a' を生成する(ステップS152)。次に、復号検証値 a' に基づき第2暗号文 $c2$ を復号して、復号乱数 $s' = c2 \text{ xor } a'$ を生成する(ステップS171)。次に、復号装置120cは、復号乱数 s' の関数値 $G(s')$ から検証値 a'' 、共有鍵 K' 及び乱数値 u' を導出する(ステップS172)。さらに、検証値 a'' を暗号化して第1再暗号文 $c1'$ を生成し(ステップS155)、 $c1' = c1$ であれば(ステップS156)、共有鍵 K' を出力する(ステップS157)。

すなわち、この復号装置120cは、以下の処理を行い、共有鍵 K' を導出する。

- (a) 秘密鍵多項式 f を用いて第1暗号文 $c1$ を復号して a' を生成する。
- (b) $s' = c2 \text{ xor } a'$ を生成する。

(c) $G(s')$ を生成し、 $G(s')$ から a' 、 K' 、 u' を生成する。

(d) 公開鍵多項式 h 、乱数値 u' を用いて a' の第1再暗号文 c_1' を生成する。

(e) $c_1' = c_1$ が成立するかどうかチェックする。成立すれば共有鍵 K' を出力する。

ここで、暗号装置110cで用いられた公開鍵多項式 h に対応する正しい秘密鍵多項式 f が復号装置120cで用いられれば、第1暗号文 c_1 は正しく復号されて、復号検証値 $a' = a$ となり、第2暗号文 c_2 と a' から生成される復号乱数 $s' = s$ となる。従って、 $G(s')$ から導出される検証値 $a' = a$ となり、共有鍵 $K' = K$ となり、乱数値 $u' = u$ となる。こうして、 $a' = a$ 及び $u' = u$ が成り立つので、 $c_1' = c_1$ が成り立ち、復号装置120cは暗号装置110cと同じ共有鍵 K を導出できることになる。

次に、復号装置120cは、インターネット130を介して暗号装置110cから共通鍵暗号文 C_i ($1 \leq i \leq n$) を受信し (ステップS108)、導出した共有鍵 K' ($=K$) を用いて、受信した共通鍵暗号文 C_i ($1 \leq i \leq n$) を共通鍵暗号方式により復号して復号文 m_i' ($1 \leq i \leq n$) を生成し (ステップS158)、復号文 m_i' ($1 \leq i \leq n$) を再生装置150へ出力する。

ここで、共通鍵暗号文生成時に用いた暗号鍵 K と復号文生成時に用いる暗号鍵 K' とは同一であるので、復号装置120cは、正しい復号文 $m_i' = m_i$ ($1 \leq i \leq n$) を得ることができる。

なお、復号エラーが発生した場合には、復号検証値 a' と検証値 a とは異なるので、第2暗号文 c_2 から得られる復号乱数 s' は s と異なる。従って、 $G(s')$ から導出される乱数値 u' 及び共有鍵 K' は、それぞれ u 、 K とは異なる。しかし、この場合、 a' 、 u' がそれぞれ a 、 u と異なるために第1再暗号文 c_1' は第1暗号文 c_1 と異なるので、復号装置120cは、共有鍵 K' を出力しない。

2. 4 実施の形態2における効果

従来のRSA-KEMアルゴリズムでは、秘密鍵を知らなければ暗号文 C から導出できない要素 s をハッシュ関数 G に入力して共有鍵 K を導出する。しかしながら、NTRU暗号を用いて、鍵カプセル化メカニズムであるRSA-KEMアルゴリズムを適用して共有鍵の配送を行おうとすると、復号エラーが発生する場合があるため、秘密鍵を用いても要素 s が導出できず、従って正しくない共有鍵 K' を導出する場合がある。

しかしながら、実施の形態2のコンテンツ配信システム、暗号装置及び復号装置は、乱数 s のハッシュ関数値 $G(s)$ から共有鍵に加えて検証値 a と乱数値 u とを生成し、復号装置が乱数値 u と公開鍵多項式 h とを用いて復号検証値 a' を再暗号化して第1再暗号文 c_1' を生成し、第1再暗号文 c_1' が第1暗号文 c_1 と同じ値でない限り共有鍵 K を出力しないので、復号エラーが発生した場合、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できる。

また、本発明による方式は、非特許文献3に記述されている証明方法と同様の方法により、理論的にその安全性が証明できる。

2. 5 変形例

上記に説明した実施の形態2は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その主旨を逸脱しない範囲において種々なる態様で実施し得るものである。実施の形態1におけるのと同様の変形を施すことができるのはもちろんであるが、以下のような場合も本発明に含まれる。

(1) 検証値 a から検証値多項式 a_p への変換は、他の変換方法でもよい。例えば、ビット列の各ビットの値と多項式の各項の係数とを1対1に対応させる関数を用いて変換してもよいし、また、ビット列の各ビットの値と多項式の各項の係数とを1対1に対応させて記憶している関数値テーブルを用いて変換してもよい。

また、乱数値 u から乱数多項式 r への変換は、他の変換方法でもよい。例えば、 u から r が一意に求まり、 d 個の次元の項の係数を「1」とし、 d 個の次元の項の係数を「-1」とし、他の次元の項の係数は「0」となるようにすれば、他の変換方法でもよい。例えば、乱数値 u を多項式に対応させる関数、又は関数値テーブルを用いて変換してもよい。

(2) 暗号化部114c及び復号化部123cで用いる公開鍵暗号は、暗号化部114cにおいて、検証値 a を公開鍵と乱数値 u を用いて暗号化して第1暗号文 c_1 を生成し、復号化部123cにおいて、第1暗号文 c_1 を秘密鍵で復号して、検証値 a と等しい復号検証値 a' を生成できればよい。従って、暗号化部114c及び復号化部123cで用いる公開鍵暗号は、NTRU暗号以外に、乱数を用いる公開鍵暗号ならばどんな暗号であってもよい。

例えば、ElGamal暗号ならば、 h 、 f をそれぞれElGamal暗号の公開鍵、秘密鍵とし、暗号化部114cにおいて、 a を h と乱数値 u を用いて暗号化して c_1 を生成し、復号化部123cにおいて、 c_1 を f を用いて復号して a' を生成すればよい。

(3) 乱数値 u は、第1関数部113c及び第2関数部126cで生成される以外にも、暗号装置110cと復号装置120cとで同じ値を得られれば、他の生成方法でもよい。

例えば、任意の関数 $Func$ に対し、 $u=Func(s)$ として暗号装置110cと復号装置120cとで同じ値を得られるようにしてもよい。すなわち、

- ・ $G(s)$ を生成し、 $G(s)$ から a 、 K を生成する。
- ・ $Func(s)$ を生成し、 $u=Func(s)$ とする。

としてもよい。

(4) さらに、乱数値 u については、第1関数部113c及び第2関数部126cで生成される以外にも、暗号装置110cと復号装置120cとで同じ値が得られればよい。暗号装置110cが乱数値 u を復号装置120cに直接送信してもよい。

すなわち、以下のように、暗号装置110cは、暗号文 C と乱数値 u とを復号装置120

bに送信してもよい。また、乱数値uを暗号化して送信してもよい。

- ・G(s)を生成し、G(s)からa、Kを生成する。
- ・暗号装置110cは、別途、乱数値uを、120bへ送信する。

(5) さらに、乱数値uについては、暗号装置110cと復号装置120cとで同じ値が得られればよい。乱数値uの一部である部分情報を第1関数部113c及び第2関数部126cで生成し、乱数値uの残りの部分情報を暗号装置110cから復号装置120cに直接送信してもよい。

例えば、以下のように、暗号装置110cは、暗号文Cと乱数値u2を復号装置120cに送信してもよい。また、暗号装置110cは、乱数値u2を暗号化して送信してもよい。

- ・G(s)を生成し、G(s)からa、K、u1を生成する。
- ・暗号装置110cは、別途、乱数値u2を復号装置120cへ送信する。
- ・暗号装置110cは、乱数値 $u = u1 \text{ xor } u2$ を生成する。

(6) 復号装置120cは、第1暗号文c1が第2関数部126cで得られる検証値a'の暗号文かどうかチェックを行い、c1がa'の暗号文であるときに共有鍵K'を用いて共通鍵暗号文Ciを復号しているが、第1暗号文c1が復号検証値a'の暗号文かどうかをチェックしてもよい。

(7) 復号装置120cは、第1暗号文c1が第2関数部126cで得られる検証値a'の暗号文かどうかチェックを行い、c1がa'の暗号文であるときに共有鍵K'を用いて共通鍵暗号文Ciを復号しているが、図12の処理系統図のステップS156に示すように、比較部127cにおいて、復号化部123cが復号したa'の値と第2関数部126cが生成したa'の値が等しいかどうかをチェックしてもよい。

(8) 復号エラー発生により暗号装置110cと復号装置120cとの間で異なる鍵が導出されるのを防止するため、第1再暗号文c1'が第1暗号文c1と同じ値かどうかを検証して共有鍵K'を出力する代わりに、暗号装置110cが乱数s、検証値a、乱数値u、共有鍵Kのいずれか1つ以上について、ハッシュ関数値を生成し、生成したハッシュ関数値を復号装置120cへ送信し、復号装置120cがこのハッシュ関数値を検証して共有鍵K'を出力するか否かを決定してもよいし、安全性を高めるために、特許文献1に開示されている方法を用いてもよい。すなわち、実施の形態1の変形例(8)を適用してもよい。

3. 実施の形態1及び実施の形態2のまとめ

以上説明したように、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出部と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して暗号化共有鍵データを生成する第1の暗号化

部とを備える。

また、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化部と、前記秘密数データを前記検証値データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化部とを備え、前記暗号化共有鍵データは、前記第1の暗号予備データと前記第2の暗号予備データから構成される。

ここで、前記第2の暗号化部は、前記秘密数データと前記検証値データの排他的論理和演算を行って前記第2の暗号予備データを生成するとしてもよい。

ここで、前記第2の暗号化部は、前記秘密数データを、前記検証値データを暗号鍵として用いて共通鍵暗号方式により暗号化して前記第2の暗号予備データを生成するとしてもよい。

ここで、前記第2の暗号化部は、前記秘密数データに前記検証値データを加算して前記第2の暗号予備データを生成するとしてもよい。

ここで、前記第2の暗号化部は、前記秘密数データに前記検証値データを乗算して前記第2の暗号予備データを生成するとしてもよい。

ここで、前記暗号化共有鍵データは、前記第1の暗号予備データと前記第2暗号予備データのビット連結データであるとしてもよい。

ここで、前記第1の暗号化部は、NTRU暗号方式により暗号化して前記暗号化共有鍵データを生成するとしてもよい。

ここで、前記第1の暗号化部は、NTRU暗号方式により暗号化して前記第1の暗号予備データを生成するとしてもよい。

ここで、前記秘密数データは、ランダムに生成される乱数であるとしてもよい。

ここで、前記共有鍵導出部は、所定の処理として、一方方向性ハッシュ関数を用いるとしてもよい。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記暗号化共有鍵データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第1の復号化部と、前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出部と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して再暗号化共有鍵データを生成する第3の暗号化部とを備え、前記暗号化共有鍵データと前記再暗号化共有鍵データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第1の暗号

予備データと第2の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第1の復号化部と、前記第2の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第2の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値検証データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化部とを備え、前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第1の暗号予備データと第2の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第1の復号化部と、前記第2の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第2の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化部とを備え、前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記共有鍵データを出力する。

ここで、前記第2の復号化部は、前記第2の暗号予備データと前記検証値データの排他的論理和演算を行って前記秘密数データを生成するとしてもよい。

ここで、前記第2の復号化部は、前記第2の暗号予備データを、前記検証値データを暗号鍵として用いて共通鍵暗号方式により復号化して前記秘密数データを生成するとしてもよい。

ここで、前記第2の復号化部は、前記第2の暗号予備データに前記検証値データを減算して前記秘密数データを生成するとしてもよい。

ここで、前記第2の暗号化部は、前記第2の暗号予備データを前記検証値データで除算して前記秘密数データ第2の秘密数データを生成するとしてもよい。

ここで、前記第1の復号化部は、NTRU暗号方式により復号化して前記共有鍵データを生成するとしてもよい。

ここで、前記第1の復号化部は、NTRU暗号方式により復号化して前記検証値データを生成するとしてもよい。

ここで、前記共有鍵導出部は、所定の処理として、一方向性ハッシュ関数を用いるとしてもよい。

また、本発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出部と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化部と、前記平文データを前記共有鍵データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化部とを備え、前記暗号文データは、前記第1の暗号予備データと前記第2の暗号予備データから構成される。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第1の暗号予備データと第2の暗号予備データから構成される暗号文データを復号して復号文データを出力する復号装置であって、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第1の復号化部と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出部と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化部とを備え、前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記第2の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号部とを備える。

また、本発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置、及び予め与えられた秘密鍵データ及び公開鍵データに基づいて暗号文データを復号して復号文データを出力する復号装置からなる暗号システムである。前記暗号装置は、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出部と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化部と、前記平文データを前記共有鍵データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化部とを備え、前記暗号文データは、前記第1の暗号予備データと前記第2の暗号予備データと前記第3の暗号予備データから構成される。前記復号装置は、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第1の復号化部と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出部と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化部とを備え、前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記第2の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号部とを備える。

以上に説明したように、本発明は、従来システムにおける問題点を鑑みて行われたもので、暗号システムにおいて、NTRU暗号を適用できる新しい鍵カプセル化メカニズムを構成することで、暗号装置と復号装置との間で異なる鍵が導出されるのを防止でき、鍵カプセル化メカニズムにより導出される鍵を用いた送信装置から受信装置への確実な暗号化通信ができる。

以上により、従来技術では達成できなかった暗号システムを提供することができ、その価

値は大きい。

4. 実施の形態3

本発明に係るさらに別の実施の形態としてのコンテンツ配信システム10d（図示していない）について説明する。

なお、コンテンツ配信システム10dは、コンテンツ配信システム10を変形したシステムである。ここでは、コンテンツ配信システム10dについて、コンテンツ配信システム10との差異点を中心に詳しく説明する。

4. 1 コンテンツ配信システム10dの構成

コンテンツ配信システム10dは、コンテンツ配信システム10と同様の構成を有しており、暗号装置110及び復号装置120に代えて、暗号装置110d及び復号装置120dを含んでいる。その他の構成については、コンテンツ配信システム10におけるものと同様であるので説明を省略する。

コンテンツ配信システム10dは、NTRU暗号を用いて鍵カプセル化メカニズムによる鍵配送を行って暗号化通信を行う暗号通信システムであり、暗号装置110dと復号装置120dとは、インターネット130を介して接続されている。

4. 2 暗号装置110dの構成

暗号装置110dは、図13に示すように、公開鍵入力部111d、乱数生成部112d、第1関数部113d、暗号化部114d、第2関数部115d、乱数マスク部116d、第1送信部117d、共通鍵暗号部118及び第2送信部119から構成されている。

暗号装置110dは、暗号装置110と同様のコンピュータシステムであり、マイクロプロセッサが、コンピュータプログラムに従って動作することにより、暗号装置110dは、その機能を達成する。

(1) 公開鍵入力部111d

公開鍵入力部111dは、メモリカード160から復号装置120の公開鍵多項式 h を読み出し、読み出した公開鍵多項式 h を暗号化部114dへ出力する。

(2) 乱数生成部112d

乱数生成部112dは、共有鍵 K を生成するための元となるシード値として、乱数 s を生成し、生成した乱数 s を第1関数部113と乱数マスク部116とへ出力する。

(3) 第1関数部113d

第1関数部113dは、乱数生成部112dから乱数 s を受け取り、受け取った乱数 s の関数値 $G(s)$ を生成し、関数値 $G(s)$ から検証値 a と共有鍵 K を生成する。ここでは、関数 G は、一方向性関数である出力長が $2k$ ビットのハッシュ関数であり、第1関数部113dは、 $G(s)$ の上位 k ビットを検証値 a とし、 $G(s)$ の下位 k ビットを共有鍵 K とする。

次に、第1関数部113dは、生成した検証値aを暗号化部114dと第2関数部115dとへ出力し、生成した共有鍵Kを共通鍵暗号部118へ出力する。

(4) 暗号化部114d

暗号化部114dは、公開鍵入力部111dから公開鍵多項式hを受け取り、第1関数部113dから検証値aを受け取り、次に示すようにして、受け取った公開鍵多項式hを用いて検証値aの第1暗号文c1を生成する。ここで、生成される第1暗号文c1は、NTRU暗号による暗号文である。

暗号化部114dは、NTRU暗号のパラメータdに対し、d個の項の各係数が「1」であり、別のd個の項の各係数が「-1」であり、その他の項の各係数が「0」となる乱数多項式rをランダムに生成する。次に、検証値aがNTRU暗号の暗号アルゴリズムEに適用できるように、検証値aを2進数表現した場合のN桁のビット列の各桁の値が、検証値多項式apの各項の係数に対応するように、検証値多項式apを生成する。例えば、検証値aの下位bビット目の値を、検証値多項式apの項 X^b の係数とする。こうして、検証値aを検証値多項式apに変換する。具体的には、検証値a=10010（ビット表現）の場合、検証値多項式 $ap = X^5 + X^2$ と変換する。次に、公開鍵多項式hを使用して、乱数多項式rを用いて検証値多項式apに前記暗号アルゴリズムEを施して、暗号文多項式である第1暗号文 $c1 = E(ap, r, h)$ を生成する。

次に、暗号化部114dは、生成した第1暗号文c1を第2関数部115dと第1送信部117dとへ出力する。

(5) 第2関数部115d

第2関数部115dは、第1関数部113dから検証値aを受け取り、暗号化部114dから第1暗号文c1を受け取り、次に示すようにして、検証値aと第1暗号文c1の関数値 $H(a, c1)$ を生成する。

ここでは、関数Hはハッシュ関数であり、一方向性関数の一種である。

第1暗号文c1は、NTRU暗号の暗号文であり多項式で表現されているので、第2関数部115dは、第1暗号文c1の各項の係数が、2進数表現した場合のN桁の第1暗号文ビット列 $c1'$ の各桁の値に対応するように、第1暗号文ビット列 $c1'$ を生成する。例えば、第1暗号文c1のb次元の項 X^b の係数を、第1暗号文ビット列 $c1'$ の下位bビット目の値とする。こうして、第1暗号文c1を第1暗号文ビット列 $c1'$ に変換する。具体的には、第1暗号文 $c1 = X^5 + X^2$ の場合、第1暗号文ビット列 $c1' = 10010$ （ビット表現）と変換する。

次に、第2関数部115dは、ハッシュ関数Hに検証値aと第1暗号文ビット列 $c1'$ とのビット結合 $a || c1'$ を入力して、関数値 $H(a, c1) = H(a || c1')$ を生成する。ここで、「||」は、ビット結合を示す演算子である。

次に、第2関数部115dは、生成した関数値 $H(a, c1)$ を乱数マスク部116dへ出力する。

(6) 乱数マスク部116d

乱数マスク部116dは、乱数生成部112dから乱数 s を受け取り、第2関数部115dから関数値 $H(a, c1)$ を受け取る。次に、第2暗号文 $c2 = s \text{ xor } H(a, c1)$ を生成し、生成した第2暗号文 $c2$ を第1送信部117dへ出力する。

なお、乱数マスク部116dは、排他的論理和 xor に代えて、共有鍵暗号アルゴリズム、加算又は乗算を用いるとしてもよい。

(7) 第1送信部117d

第1送信部117dは、暗号化部114dから第1暗号文 $c1$ を受け取り、乱数マスク部116dから第2暗号文 $c2$ を受け取り、受け取った第1暗号文 $c1$ と第2暗号文 $c2$ とを、インターネット130を介して、復号装置120dへ送信する。

(8) 共通鍵暗号部118及び第2送信部119

共通鍵暗号部118及び第2送信部119は、以下に示す点を除いて、それぞれ、暗号装置110に含まれている共通鍵暗号部118及び第2送信部119と同じである。

共通鍵暗号部118は、第1関数部113dから共有鍵 K を受け取る。

4. 3 復号装置120dの構成

復号装置120dは、図14に示すように、秘密鍵入力部121d、第1受信部122d、復号化部123d、第3関数部124d、乱数マスク除去部125d、第4関数部126d、比較部127d、共通鍵復号部128及び第2受信部129から構成されている。

復号装置120dは、復号装置120と同様のコンピュータシステムであり、マイクロプロセッサが、コンピュータプログラムに従って動作することにより、復号装置120dは、その機能を達成する。

なお、共通鍵復号部128及び第2受信部129は、それぞれ、復号装置120に含まれている共通鍵復号部128及び第2受信部129と同じであるので、ここでは、説明を省略する。

(1) 秘密鍵入力部121d

秘密鍵入力部121dは、メモリカード170から復号装置120dの秘密鍵多項式 f を読み出し、読み出した秘密鍵多項式 f を復号化部123dへ出力する。

(2) 第1受信部122d

第1受信部122dは、インターネット130を介して暗号装置110dから第1暗号文 $c1$ と第2暗号文 $c2$ とを受け取り、受け取った第1暗号文 $c1$ を復号化部123dと第3関数部124dとへ出力し、受け取った第2暗号文 $c2$ を乱数マスク除去部125dへ出力する。

なお、乱数マスク部116dが、排他的論理和に代えて、共有鍵暗号アルゴリズム、加算又は乗算を用いる場合において、乱数マスク除去部125dは、それぞれ、共有鍵暗号アルゴリズムに対応する共有鍵復号アルゴリズム、減算、又は除算を用いるとしてもよい。

(3) 復号化部123d

復号化部123dは、秘密鍵入力部121dから秘密鍵多項式 f を受け取り、第1受信部122dから第1暗号文 c_1 を受け取り、次に示すようにして、秘密鍵多項式 f を用いて、第1暗号文 c_1 を復号して復号検証値 a' を生成する。ここでは、復号検証値 a' はNTRU暗号による復号文である。

復号化部123dは、秘密鍵多項式 f を使用して、第1暗号文 c_1 に前記復号アルゴリズム D を施して、復号検証値多項式 $a_p' = D(c_1, f)$ を生成する。次に、復号検証値多項式 a_p' は、NTRU暗号の復号文であり多項式で表現されているので、復号化部123dは、復号検証値多項式 a_p' の各係数が、復号検証値 a' を2進数表現した場合の N 桁のビット列の各桁の数に対応するように、復号検証値 a' を生成する。例えば、復号検証値多項式 a_p' の b 次元の項 X^b の係数を、復号検証値 a' の下位 b ビット目の値とする。こうして、復号検証値多項式 a_p' を復号検証値 a' に変換する。具体的には、復号検証値多項式 $a_p' = X^5 + X^2$ の場合、復号検証値 $a' = 10010$ （ビット表現）に変換する。

次に、復号化部123dは、生成した復号検証値 a' を第3関数部124dと比較部127dとへ出力する。

(4) 第3関数部124d

第3関数部124dは、第2関数部115dが有する関数と同じ関数 H のアルゴリズムを有している。

第3関数部124dは、第1受信部122dから第1暗号文 c_1 を受け取り、復号化部123dから復号検証値 a' を受け取る。次に、第2関数部115dと同様にして、検証値 a' と第1暗号文 c_1 との関数値 $H(a', c_1)$ を生成し、生成した関数値 $H(a', c_1)$ を乱数マスク除去部125dへ出力する。

(5) 乱数マスク除去部125d

乱数マスク除去部125dは、第1受信部122dから第2暗号文 c_2 を受け取り、第3関数部124dからハッシュ関数値 $H(a', c_1)$ を受け取り、次に、復号乱数 $s' = c_2 \oplus H(a', c_1)$ を生成し、生成した復号乱数 s を第4関数部126dへ出力する。

(6) 第4関数部126d

第4関数部126dは、第1関数部113dが有する関数と同じ関数 G のアルゴリズムを有している。

第4関数部126dは、乱数マスク除去部125dから復号乱数 s' を受け取り、復号乱数 s' のハッシュ関数値 $G(s')$ を生成する。次に、第1関数部113dと同様にして、関

数値G (s') から検証値a'' と共有鍵K' とを生成し、生成した検証値a'' と共有鍵K' とを比較部127dへ出力する。

(7) 比較部127d

比較部127dは、復号化部123dから復号検証値a'を受け取り、第4関数部126dから検証値a'' と共有鍵K' とを受け取り、次に、復号検証値a' と検証値a'' が等しいかどうかチェックを行い、復号検証値a' と検証値a'' とが等しければ、共有鍵K' を共通鍵復号部128へ出力する。

(8) 共通鍵復号部128及び第2受信部129

共通鍵復号部128は、比較部127dから共有鍵K' を受け取る。

その他の点については、共通鍵復号部128は、復号装置120に含まれている共通鍵復号部128と同じであるので、ここでは、説明を省略する。

また、第2受信部129は、復号装置120に含まれている第2受信部129と同じであるので、ここでは、説明を省略する。

4. 4 コンテンツ配信システム10dの動作

コンテンツ配信システム10dの動作について、図15に示すフローチャート及び図16に示す処理系統図を用いて説明する。

公開鍵入力部111dは、メモリカード160から復号装置120dの公開鍵多項式hを受け取り、公開鍵多項式hを暗号化部114dへ出力する(ステップS201)。

次に、乱数生成部112dは、乱数sを生成して、乱数sを第1関数部113dと乱数マスク部116dとへ出力する(ステップS202)。

次に、第1関数部113dは、乱数生成部112dから乱数sを受け取り、乱数sの関数値G(s)を生成する(ステップS203)。そして、第1関数部113dは、関数値G(s)から検証値aと共有鍵Kを生成して、検証値aを暗号化部114dと第2関数部115dとへ出力し、共有鍵Kを共通鍵暗号部118へ出力する(ステップS204)。

次に、暗号化部114dは、公開鍵入力部111dから公開鍵多項式hを受け取り、第1関数部113dから検証値aを受け取る。そして、暗号化部114dは、公開鍵多項式hを用いて検証値aの第1暗号文c1を生成し、第1暗号文c1を第2関数部115dと第1送信部117dとへ出力する(ステップS205)。

次に、第2関数部115dは、第1関数部113dから検証値aを受け取り、暗号化部114dから第1暗号文c1を受け取り、検証値aと第1暗号文c1との関数値H(a, c1)を生成し、関数値H(a, c1)を乱数マスク部116へ出力する(ステップS206)。

次に、乱数マスク部116dは、乱数生成部112dから乱数sを受け取り、第2関数部115dから関数値H(a, c1)を受け取り、乱数マスク部116dは、第2暗号文c2 = s xor H(a, c1)を生成し、第2暗号文c2を第1送信部117dへ出力する

(ステップS207)。

次に、第1送信部117dは、暗号化部114dから第1暗号文 c_1 を受け取り、乱数マスク部116dから第2暗号文 c_2 を受け取り、第1暗号文 c_1 と第2暗号文 c_2 とをインターネット130を介して復号装置120dへ送信する(ステップS208)。

次に、共通鍵暗号部118は、コンテンツサーバ装置140から複数の平文 m_i ($1 \leq i \leq n$)を受け取り、第1関数部113dから共有鍵 K を受け取り、共有鍵 K を使用して平文 m_i ($1 \leq i \leq n$)に共通鍵暗号アルゴリズム Sym を施して、共通鍵暗号文 $C_i = Sym(m_i, K)$ ($1 \leq i \leq n$)を生成し、共通鍵暗号文 C_i ($1 \leq i \leq n$)を第2送信部119へ出力する(ステップS209)。

次に、第2送信部119は、共通鍵暗号部118から共通鍵暗号文 C_i ($1 \leq i \leq n$)を受け取り、インターネット130を介して復号装置120dへ送信し(ステップS210)、処理を終了する。

一方、秘密鍵入力部121dは、メモリカード170から復号装置120dの秘密鍵多項式 f を受け取り、秘密鍵多項式 f を復号化部123へ出力する(ステップS251)。

次に、第1受信部122dは、インターネット130を介して暗号装置110dから第1暗号文 c_1 と第2暗号文 c_2 とを受け取り、第1暗号文 c_1 を復号化部123dと第3関数部124dとへ出力し、第2暗号文 c_2 を乱数マスク除去部125dへ出力する(ステップS208)。

次に、復号化部123dは、秘密鍵入力部121から秘密鍵多項式 f を受け取り、第1受信部122dから第1暗号文 c_1 を受け取り、次に、秘密鍵多項式 f を用いて、第1暗号文 c_1 を復号して復号検証値 a' を生成し、復号検証値 a' を第3関数部124dと比較部127dへ出力する(ステップS252)。

次に、第3関数部124dは、第1受信部122dから第1暗号文 c_1 を受け取り、復号化部123dから復号検証値 a' を受け取り、次に、第2関数部115dと同様にして、検証値 a' と第1暗号文 c_1 の関数値 $H(a', c_1)$ を生成し、関数値 $H(a', c_1)$ を乱数マスク除去部125dへ出力する(ステップS253)。

次に、乱数マスク除去部125dは、第1受信部122dから第2暗号文 c_2 を受け取り、第3関数部124dからハッシュ関数値 $H(a', c_1)$ を受け取り、次に、復号乱数 $s' = c_2 \text{ xor } H(a', c_1)$ を生成し、復号乱数 s を第4関数部126dへ出力する(ステップS254)。

次に、第4関数部126dは、乱数マスク除去部125から復号乱数 s' を受け取り、復号乱数 s' のハッシュ関数値 $G(s')$ を生成し(ステップS255)、第1関数部113dと同様にして、関数値 $G(s')$ から検証値 a'' と共有鍵 K' とを生成して、検証値 a'' と共有鍵 K' とを比較部127dへ出力する(ステップS256)。

次に、比較部127dは、復号化部123から復号検証値 a' を受け取り、第4関数部126dから検証値 a'' と共有鍵 K' を受け取り、復号検証値 a' と検証値 a'' とが等しいかどうかチェックを行い、等しくなければ（ステップS257）、処理を終了する。

復号検証値 a' と検証値 a'' とが等しければ（ステップS257）、比較部127dは、共有鍵 K' を共通鍵復号部128へ出力する（ステップS258）。

次に、第2受信部129は、インターネット130を介して暗号装置110dから暗号文 C_i ($1 \leq i \leq n$)を受信し、共通鍵復号部128へ出力する（ステップS210）。

次に、共通鍵復号部128は、比較部127dから共有鍵 K' を受け取り、第2受信部129から共通鍵暗号文 C_i ($1 \leq i \leq n$)を受け取り、共有鍵 K' を使用して共通鍵暗号文 C_i ($1 \leq i \leq n$)に共通鍵暗号アルゴリズム Sym を施して、復号文 $m_i' = Sym(C_i, K)$ ($1 \leq i \leq n$)を生成し、復号文 m_i' ($1 \leq i \leq n$)を外部へ出力し（ステップS259）、処理を終了する。

4. 5 コンテンツ配信システム10dの動作検証

以下に、コンテンツ配信システム10dの全体の動作について説明する。

暗号装置110dは、復号装置120dの公開鍵多項式 h を入力とし、乱数 s を生成して、関数値 $G(s)$ から検証値 a と共有鍵 K を導出する。次に、暗号装置110dは、検証値 a を公開鍵多項式 h を用いてNTRU暗号で暗号化して第1暗号文 c_1 を生成し、検証値 a と第1暗号文 c_1 から関数値 $H(a, c_1)$ を生成し、乱数 s と関数値 $H(a, c_1)$ から第2暗号文 $c_2 = s \text{ xor } H(a, c_1)$ を生成する。次に、暗号装置110dは、第1暗号文 c_1 と第2暗号文 c_2 をインターネット130を介して復号装置120dへ送信する。

すなわち、この暗号装置110dは、以下の処理を行い、暗号文 $C = (c_1, c_2)$ を復号装置120dへ送信する。

- ・乱数 s を生成する。
- ・ $G(s)$ を生成し、 $G(s)$ から a 、 K を生成する。
- ・公開鍵多項式 h を用いて検証値 a の第1暗号文 c_1 を生成する。
- ・ $c_2 = s \text{ xor } H(a, c_1)$ を生成する。
- ・共有鍵 K と暗号文 $C = (c_1, c_2)$ を出力する。

次に、暗号装置110dは、導出した共有鍵 K を用いて、コンテンツサーバ装置140から入力された平文 m_i ($1 \leq i \leq n$)を共通鍵暗号で暗号化して暗号文 C_i ($1 \leq i \leq n$)を生成し、インターネット130を介して復号装置120dへ送信する。

一方、復号装置120dは、復号装置120dの秘密鍵多項式 f を入力とし、インターネット130を介して暗号装置110dから第1暗号文 c_1 と第2暗号文 c_2 とを受信し、第1暗号文 c_1 を秘密鍵多項式 f を用いて復号して復号検証値 a' を生成する。復号検証値 a' と第1暗号文 c_1 から関数値 $H(a', c_1)$ を生成し、第2暗号文 c_2 と関数値 $H(a'$,

c1) から復号乱数 $s' = c2 \text{ xor } H(a', c1)$ を生成する。次に、復号装置120dは、復号乱数 s' の関数値 $G(s')$ から検証値 a'' と共有鍵 K' を導出し、検証値 $a'' = a'$ であれば共有鍵 K' を出力する。

すなわち、この復号装置120dは、以下の処理を行い、共有鍵 K' を導出する。

- ・秘密鍵多項式 f を用いて第1暗号文 $c1$ を復号して a' を生成する。
- ・ $s' = c2 \text{ xor } H(a', c1)$ を生成する。
- ・ $G(s')$ を生成し、 $G(s')$ から a'' 、 K' を生成する。
- ・ $a'' = a'$ が成立するかどうかチェックする。成立すれば共有鍵 K' を出力する。

ここで、暗号装置110dで用いられた公開鍵多項式 h に対応する正しい秘密鍵多項式 f が復号装置120dで用いられれば、第1暗号文 $c1$ は正しく復号されて、復号検証値 $a' = a$ となり、第2暗号文 $c2$ と $H(a', c1)$ から生成される復号乱数 $s' = s$ となる。従って、 $G(s')$ から導出される検証値 $a'' = a$ となり、共有鍵 $K' = K$ となる。そして、 $a'' = a'$ が成り立つので、復号装置120dは暗号装置110dと同じ共有鍵 K を導出できることになる。

次に、復号装置120dは、導出した共有鍵 $K' (=K)$ を用いて、インターネット130を介して暗号装置110dから共通鍵暗号文 $C_i (1 \leq i \leq n)$ を受け取り、受け取った共通鍵暗号文 $C_i (1 \leq i \leq n)$ を共通鍵暗号で復号して復号文 $m_i' (1 \leq i \leq n)$ を生成して再生装置150へ出力する。

ここで、共通鍵暗号文生成時に用いた暗号鍵 K と復号文生成時に用いる暗号鍵 K' は同一であるので、復号装置120dは、正しく $m_i' = m_i (1 \leq i \leq n)$ を得ることができる。

4.6 実施の形態3における効果

従来のPSEC-KEMアルゴリズムでは、ハッシュ関数 H の入力に $a * P$ 、 $a * W$ を用い、秘密鍵を用いずに $a * P$ から $a * W$ を計算することが困難なDiffie-Hellman問題を用いて、最終的に共有鍵 K を導出することにより、秘密鍵を知らなければその共有鍵 K を導出できないようにしている。従って、NTRU暗号をはじめ、Diffie-Hellman問題を利用しない他の公開鍵暗号は、Diffie-Hellman問題の $a * P$ 、 $a * W$ に相当するものがないため、PSEC-KEMアルゴリズムを適用できないという問題点がある。

しかしながら、本発明のコンテンツ配信システム、暗号装置及び復号装置は、ハッシュ関数 H の入力を検証値 a とその暗号文 $c1$ としているので、PSEC-KEMアルゴリズムを適用して、NTRU暗号や他の公開鍵暗号を利用できる。

なお、NTRU暗号では、公開鍵を用いて平文を暗号化して暗号文を生成し、正規の秘密鍵を用いて暗号文を復号して復号文を生成しても、復号文が元の平文と異なる場合が発生す

る（例えば、非特許文献2参照）。このような復号エラーが発生すると、復号装置は誤った復号検証値 a' を得ることになるが、 $G(s')$ から得られる検証値 a'' は a' と等しくならないために、共有鍵 K' を出力しない。従って、復号エラーが発生しても、暗号装置と復号装置との間で誤った鍵を共有することを防止できるという効果がある。

また、復号装置において、再度暗号文を生成する処理を行わないので、従来技術と比較すると、演算量を削減することができる。

これにより、NTRU暗号を用いて鍵カプセル化メカニズムを構成することができ、暗号装置と復号装置との間でNTRU暗号を用いて鍵配送が行えるようになる。

また、本発明による方式は、非特許文献3に記述されている証明方法と同様の方法により、理論的にその安全性が証明できる。

4. 7 変形例

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

(1) 用いるNTRU暗号のパラメータ $N=167$ に限定されない。パラメータ N は、他の値をとるとしてもよい。

(2) 暗号化部114d、第2関数部115d、復号化部123d及び第3関数部124dで行われるビット列と多項式との変換方法は、この方法に限られず他の変換方法でもよい。

例えば、ビット列と多項式を1対1に対応させる関数、又は関数値のテーブルを用いて変換してもよい。

また、例えば、実施の形態2の変形例(1)に述べた変換方法を用いて変換してもよい。

(3) 暗号化部114d及び復号化部123dで用いる公開鍵暗号方式は、暗号化部114dにおいて、検証値 a を公開鍵で暗号化して第1暗号文 c_1 を生成し、復号化部123dにおいて、第1暗号文 c_1 を秘密鍵で復号して、検証値 a と等しい復号検証値 a' を生成できればよい。

従って、暗号化部114d、復号化部123dで用いる公開鍵暗号は、NTRU暗号以外に、どんな公開鍵暗号でも利用できる。

例えば、RSA暗号を採用するならば、 h 、 f をそれぞれRSA暗号の公開鍵、秘密鍵とし、暗号化部114dにおいて、 a を h を用いて暗号化して c_1 を生成し、復号化部123dにおいて、 c_1 を f を用いて復号して a' を生成すればよい。

また、例えば、ElGamal暗号採用するならば、 h 、 f をそれぞれElGamal暗号の公開鍵、秘密鍵とし、暗号化部114dにおいて、乱数 r を生成して a を h と r を用いて暗号化して c_1 を生成し、復号化部123dにおいて、 c_1 を f を用いて復号して a' を生成すればよい。

なお、RSA暗号やElGamal暗号について非特許文献1に詳細に記載されているため、ここでは説明を省略する。

(4) 第1関数部113dは、関数値 $G(s)$ の上位 k ビットを検証値 a をして下位 k ビットを共有鍵 K とする以外に、関数値 $G(s)$ から検証値 a と共有鍵 K を導出すれば他の方法でもよい。

(5) 第2関数部115dは、検証値 a と第1暗号文 $c1$ から関数値 $H(a, c1)$ を導出すれば他の方法でもよい。

例えば、任意の2項演算 $\#$ に対し、 $a \# c1$ を関数 H に入力して関数値を導出してもよい。なお、NTRU暗号では第1暗号文 $c1$ は多項式であるので、第1暗号文 $c1$ から第1暗号文ビット列 $c1'$ に変換し、 $a \# c1'$ を関数 H に入力して関数値を導出してもよい。

(6) さらに、第2関数部115dは、検証値 a を用いて関数値を導出すれば、他の方法でもよい。

例えば、第2関数部115dは、 $H(a)$ を出力してもよいし、検証値 a をそのまま出力してもよい。すなわち、暗号装置110dにおいて、第2暗号文 $c2$ を

- ・ $c2 = s \text{ xor } H(a)$ 、又は
- ・ $c2 = s \text{ xor } a$ として導出してもよい。

これらの場合において、復号装置120dの第3関数部124dは、それぞれ、

- ・ $H(a')$ 又は
- ・ a'

を出力する。

(7) 乱数マスク部116dは、乱数 s と関数値 $H(a, c1)$ とから第2暗号文 $c2$ を導出し、乱数マスク除去部125dは、第2暗号文 $c2$ と関数値 $H(a, c1)$ とから乱数 s が導出できれば、他の方法でもよい。

例えば、乱数マスク部116dは、第2暗号文 $c2$ を

- ・ $c2 = s + H(a, c1)$ 、又は
- ・ $c2 = s \cdot H(a, c1)$

として導出してもよい。

5. 実施の形態4

本発明に係るさらに別の実施の形態としてのコンテンツ配信システム10e（図示していない）について説明する。

コンテンツ配信システム10eは、実施の形態3に示すコンテンツ配信システム10dを基本として、これを変形したシステムであり、暗号装置が、関数値 $G(s)$ から検証値 a と共有鍵 K の他に乱数値 u を生成し、乱数値 u を用いて検証値 a を暗号化して第1暗号文 $c1$ を生成する点と、復号装置が、共有鍵 K を出力するときの判断の方法とにおいて、コンテン

ツ配信システム10dと異なる。

ここでは、コンテンツ配信システム10eについて、コンテンツ配信システム10dとの差異点を中心に詳しく説明する。

5. 1 コンテンツ配信システム10eの構成

コンテンツ配信システム10eは、コンテンツ配信システム10dと同様の構成を有しており、暗号装置110d及び復号装置120dに代えて、暗号装置110e及び復号装置120eを含んでいる。その他の構成については、コンテンツ配信システム10dにおけるものと同様であるので説明を省略する。

コンテンツ配信システム10eは、NTRU暗号を用いて鍵配送を行うシステムである。暗号装置110eと復号装置120eとは、インターネット130を介して接続されている。

5. 2 暗号装置110eの構成

暗号装置110eは、図17に示すように、公開鍵入力部111d、乱数生成部112d、第1関数部113e、暗号化部114e、第2関数部115d、乱数マスク部116d、第1送信部117d、共通鍵暗号部118及び第2送信部119から構成されている。

公開鍵入力部111d、乱数生成部112d、第2関数部115d、乱数マスク部116d、第1送信部117d、共通鍵暗号部118及び第2送信部119は、暗号装置110dを構成する構成要素と同一であるので、説明を省略し、ここでは、暗号装置110dを構成する構成要素と異なる第1関数部113e及び暗号化部114eについてその構成と動作を説明する。

(1) 第1関数部113e

第1関数部113eは、乱数生成部112dから乱数 s を受け取り、受け取った乱数 s の関数値 $G(s)$ を生成する。次に、以下に示すようにして、生成した関数値 $G(s)$ から検証値 a と共有鍵 K と乱数値 u とを生成する。

ここで、関数 G は、出力長が $3k$ ビットのハッシュ関数であり、第1関数部113eは、 $G(s)$ の上位 k ビットを検証値 a とし、 $G(s)$ の中間の k ビットを共有鍵 K とし、 $G(s)$ の下位 k ビットを乱数値 u とする。

次に、第1関数部113eは、生成した検証値 a を暗号化部114eと第2関数部115dとへ出力し、生成した共有鍵 K を共通鍵暗号部118へ出力し、生成した乱数値 u を暗号化部114eへ出力する。

(2) 暗号化部114e

暗号化部114eは、公開鍵入力部111dから公開鍵多項式 h を受け取り、第1関数部113eから検証値 a と乱数値 u とを受け取る。次に、以下に示すようにして、公開鍵多項式 h と乱数値 u とを用いて検証値 a の第1暗号文 c_1 を生成する。ここで、第1暗号文 c_1 は、NTRU暗号による暗号文である。また、乱数値 u は、ブラインド値であり、暗号化の

対象である検証値 a を不明瞭にするために用いられる。

暗号化部 114 e は、NTRU 暗号のパラメータ d に対し、 d 個の項の各係数が「1」であり、他の d 個の項の各係数が「-1」であり、残りの項の各係数が「0」となる乱数多項式 r を乱数値 u から一意に求まるように生成する。

具体的には、例えば、暗号化部 114 e は、乱数値 u を擬似乱数系列の初期値（乱数シード）として設定し、 $\{0, 1, \dots, N-1\}$ から重複しない $2d$ 個の擬似乱数を生成し、最初の d 個の擬似乱数により示される次元の項の係数を「1」とし、次の d 個の擬似乱数により示される次元の項の係数を「-1」とし、残りの次元の項の係数を「0」とすることにより、乱数多項式 r を生成する。

次に、暗号化部 114 e は、生成した乱数多項式 r を用いて、暗号化部 114 d と同様に、第 1 暗号文 $c_1 = E(a_p, r, h)$ を生成する。

次に、暗号化部 114 e は、生成した第 1 暗号文 c_1 を第 2 関数部 115 d と第 1 送信部 117 d とへ出力する。

5.3 復号装置 120 e の構成

復号装置 120 e は、図 18 に示すように、秘密鍵入力部 121 e、復号化部 123 e、第 3 関数部 124 d、乱数マスク除去部 125 d、第 4 関数部 126 e、比較部 127 e、共通鍵復号部 128 及び第 2 受信部 129 から構成されている。

ここで、第 3 関数部 124 d、乱数マスク除去部 125 d、共通鍵復号部 128 及び第 2 受信部 129 については、復号装置 120 d に含まれている各構成要素と同一であるので、説明を省略し、復号装置 120 d に含まれている各構成要素と異なる秘密鍵入力部 121 e、復号化部 123 e、第 4 関数部 126 e 及び第 2 比較部 127 e についてその構成と動作を説明する。

(1) 秘密鍵入力部 121 e

秘密鍵入力部 121 e は、メモ리카ード 170 から復号装置 120 e の秘密鍵多項式 f と公開鍵多項式 h とを受け取り、秘密鍵多項式 f を復号化部 123 e へ出力し、公開鍵多項式 h を比較部 127 e へ出力する。

(2) 復号化部 123 e

復号化部 123 e は、秘密鍵入力部 121 e から秘密鍵多項式 f を受け取り、第 1 受信部 122 d から第 1 暗号文 c_1 を受け取る。次に、秘密鍵多項式 f を用いて、第 1 暗号文 c_1 を復号して復号検証値 a' を生成し、生成した復号検証値 a' を第 3 関数部 124 d へ出力し、受け取った第 1 暗号文 c_1 を比較部 127 e へ出力する。

(3) 第 4 関数部 126 e

第 4 関数部 126 e は、第 1 関数部 113 e が有する関数と同じ関数 G によるアルゴリズムを有している。

第4関数部126eは、乱数マスク除去部125dから復号乱数 s' を受け取り、受け取った復号乱数 s' のハッシュ関数値 $G(s')$ を生成する。次に、第1関数部113eと同様にして、関数値 $G(s')$ から検証値 a'' と共有鍵 K' と乱数値 u' とを生成し、検証値 a'' と共有鍵 K' と乱数値 u' とを比較部127eへ出力する。

(4) 比較部127e

比較部127eは、図18に示すように、比較演算部127p及び暗号化部127qから構成されている。

暗号化部127qは、秘密鍵入力部121eから公開鍵多項式 h を受け取り、第4関数部126eから検証値 a'' と乱数値 u' とを受け取る。次に、受け取った公開鍵多項式 h と乱数値 u' とを用いて、暗号化部114dと同様にして、受け取った検証値 a'' を暗号化して第1再暗号文 $c1'$ を生成し、生成した第1再暗号文 $c1'$ を比較演算部127pへ出力する。

比較演算部127pは、復号化部123bから第1暗号文 $c1$ を受け取り、暗号化部127qから第1再暗号文 $c1'$ を受け取る。次に、受け取った第1暗号文 $c1$ と第1再暗号文 $c1'$ とを比較して、 $c1' = c1$ であるか否かを判断する。 $c1' = c1$ であれば、受け取った共有鍵 K' を共通鍵復号部128へ出力し、 $c1' \neq c1$ でなければ、受け取った共有鍵 K' を出力しない。

5. 4 コンテンツ配信システム10eの動作検証

以下に、コンテンツ配信システム10eの全体の動作について、図19に示す処理系統図を用いて説明する。

暗号装置110eは、復号装置120eの公開鍵多項式 h を受け取り(ステップS201)、乱数 s を生成し(ステップS202)、関数値 $G(s)$ を生成し(ステップS203)、関数値 $G(s)$ から検証値 a 、共有鍵 K 及び乱数値 u を導出する(ステップS204e)。次に、暗号装置110eは、検証値 a を、公開鍵多項式 h 及び乱数値 u を用いてNTRU暗号で暗号化して第1暗号文 $c1$ を生成し(ステップS205)、検証値 a と第1暗号文 $c1$ から関数値 $H(a, c1)$ を生成し(ステップS206)、乱数 s と関数値 $H(a, c1)$ から第2暗号文 $c2 = s \text{ xor } H(a, c1)$ を生成する(ステップS207)。次に、暗号装置110bは、第1暗号文 $c1$ と第2暗号文 $c2$ とをインターネット130を介して復号装置120eへ送信する(ステップS208)。

すなわち、この暗号装置110eは、以下の処理(a)～(d)を行い、暗号文 $C = (c1, c2)$ を復号装置120eへ送信する。

(a) 乱数 s を生成する。

(b) $G(s)$ を生成し、 $G(s)$ から a 、 K 、 u を生成する。

(c) 公開鍵多項式 h 、乱数値 u を用いて検証値 a の第1暗号文 $c1$ を生成する。

(d) $c2 = s \text{ xor } H(a, c1)$ を生成する。

次に、暗号装置110eは、導出した共有鍵Kを用いて、コンテンツサーバ装置140から入力された平文 m_i ($1 \leq i \leq n$) を共通鍵暗号で暗号化して暗号文 C_i ($1 \leq i \leq n$) を生成し(ステップS209)、インターネット130を介して復号装置120eへ送信する(ステップS210)。

一方、復号装置120eは、復号装置120eの秘密鍵多項式f及び公開鍵多項式hを受け取り(ステップS251、ステップS251e)、インターネット130を介して暗号装置110eから第1暗号文 $c1$ と第2暗号文 $c2$ を受信し(ステップS208)、第1暗号文 $c1$ を秘密鍵多項式fを用いて復号して復号検証値 a' を生成する(ステップS252)。次に、復号検証値 a' と第1暗号文 $c1$ から関数値 $H(a', c1)$ を生成し(ステップS253)、第2暗号文 $c2$ と関数値 $H(a', c1)$ から復号乱数 $s' = c2 \text{ xor } H(a', c1)$ を生成する(ステップS254)。次に、復号装置120eは、復号乱数 s' の関数値 $G(s')$ を生成し(ステップS255)、生成した関数値 $G(s')$ から検証値 a'' 、共有鍵 K' 及び乱数値 u' を導出する(ステップS256e)。次に、検証値 a'' を暗号化して第1再暗号文 $c1'$ を生成し(ステップS261)、 $c1' = c1$ であれば(ステップS257e)、共有鍵 K' を出力する(ステップS258)。

すなわち、復号装置120eは、以下の処理(a)～(e)を行い、共有鍵 K' を導出する。

(a) 秘密鍵多項式fを用いて第1暗号文 $c1$ を復号して a' を生成する。

(b) $s' = c2 \text{ xor } H(a', c1)$ を生成する。

(c) $G(s')$ を生成し、 $G(s')$ から a'' 、 K' 、 u' を生成する。

(d) 公開鍵多項式h及び乱数値 u' を用いて a'' の第1再暗号文 $c1'$ を生成する。

(e) $c1' = c1$ が成立するかどうかチェックする。成立すれば共有鍵 K' を出力する。

ここで、暗号装置110eで用いられた公開鍵多項式hに対応する正しい秘密鍵多項式fが復号装置120eで用いられれば、第1暗号文 $c1$ は正しく復号されて、復号検証値 $a' = a$ となり、第2暗号文 $c2$ と $H(a', c1)$ から生成される復号乱数 $s' = s$ となる。従って、 $G(s')$ から導出される検証値 $a'' = a$ となり、共有鍵 $K' = K$ となり、乱数値 $u' = u$ となる。そして、 $a'' = a$ 及び $u' = u$ が成り立つので、 $c1' = c1$ が成り立ち、復号装置120eは暗号装置110eと同じ共有鍵Kを導出できることになる。

次に、復号装置120eは、導出した共有鍵 K' ($=K$)を用いて、インターネット130を介して暗号装置110eから共通鍵暗号文 C_i ($1 \leq i \leq n$)を受信し(ステップS210)、受信した共通鍵暗号文 C_i ($1 \leq i \leq n$)を共通鍵暗号で復号して復号文 m_i' ($1 \leq i \leq n$)を生成し(ステップS259)、生成した復号文 m_i' ($1 \leq i \leq n$)を再生装置150へ出力する。

ここで、共通鍵暗号文生成時に用いた暗号鍵 K と復号文生成時に用いる暗号鍵 K' とは同一であるので、復号装置120eは、正しく $mi' = mi$ ($1 \leq i \leq n$)を得ることができる。

5. 5 コンテンツ配信システム10eにおける効果

従来のPSEC-KEMアルゴリズムでは、ハッシュ関数 H の入力に $a * P$ 、 $a * W$ を用い、秘密鍵を用いずに $a * P$ から $a * W$ を計算することが困難なDiffie-Hellman問題を用いて、最終的に共有鍵 K を導出することにより、秘密鍵を知らなければその共有鍵 K を導出できないようにしている。従って、NTRU暗号をはじめ、Diffie-Hellman問題を利用しない他の公開鍵暗号では、Diffie-Hellman問題の $a * P$ 、 $a * W$ に相当するものがないため、PSEC-KEMアルゴリズムを適用できないという問題点がある。

しかしながら、本発明のコンテンツ配信システム、暗号装置及び復号装置では、ハッシュ関数 H の入力を検証値 a とその暗号文 c_1 としたので、実施の形態3と同様に、NTRU暗号や他の公開鍵暗号を適用できる。

なお、復号エラーが発生すると、復号装置は誤った復号検証値 a' を得ることになるが、 c_1' は c_1 と等しくならないために、共有鍵 K' を出力しない。従って、復号エラーが発生しても、暗号装置と復号装置との間で誤った鍵を共有することを防止できるという効果もある。

これにより、NTRU暗号を用いて鍵カプセル化メカニズムを構成することができ、暗号装置と復号装置との間でNTRU暗号を用いて鍵配送が行えるようになる。

また、本発明による方式は、非特許文献3に記述されている証明方法と同様の方法により、理論的にその安全性が証明できる。

5. 6 変形例

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その主旨を逸脱しない範囲において種々なる態様で実施し得るものである。実施の形態3におけるのと同様の変形を施すことができるのはもちろんであるが、以下のような場合も本発明に含まれる。

(1) 暗号化部114eで行われる乱数値 u から乱数多項式 r への変換方法は、この方法に限られず u から r が一意に求まれば他の変換方法でもよい。例えば、乱数値 u を多項式に対応させる関数、又は関数値テーブルを用いて変換してもよい。

また、例えば、実施の形態2の変形例(1)に述べた変換方法を用いて変換してもよい。

(2) 暗号化部114e及び復号化部123eで用いる公開鍵暗号は、暗号化部114eにおいて、検証値 a を公開鍵と乱数値 u とを用いて暗号化して第1暗号文 c_1 を生成し、復号化部123eにおいて、第1暗号文 c_1 を秘密鍵で復号して、検証値 a と等しい復号検証

値 a' を生成できればよい。従って、暗号化部114e及び復号化部123eで用いる公開鍵暗号は、NTRU暗号以外に、乱数を用いる公開鍵暗号ならばどんな暗号でも利用できる。

例えば、ElGamal暗号ならば、 h 、 f をそれぞれElGamal暗号の公開鍵、秘密鍵とし、暗号化部114eにおいて、 a を h と乱数値 u とを用いて暗号化して $c1$ を生成し、復号化部123eにおいて、 $c1$ を f を用いて復号して a' を生成すればよい。

(3) 乱数値 u は、第1関数部113e及び第4関数部126eで生成される以外にも、暗号装置110eと復号装置120eとで同じ値を得られれば、他の生成方法でもよい。

例えば、任意の関数Funcに対し、 $u = \text{Func}(s)$ として暗号装置110eと復号装置120eとで同じ値を得られるようにしてもよい。すなわち、

- ・ $G(s)$ を生成し、 $G(s)$ から a 、 K を生成する。
- ・ $\text{Func}(s)$ を生成し、 $u = \text{Func}(s)$ とする。

としてもよい。

(4) さらに、乱数値 u は、第1関数部113e及び第4関数部126eで生成される以外にも、暗号装置110eと復号装置120eとで同じ値を得られればよい。暗号装置110eが乱数値 u を復号装置120eに直接送信してもよい。

すなわち、以下のように、暗号文 C と乱数値 u とを復号装置120eに送信してもよい。

- ・ $G(s)$ を生成し、 $G(s)$ から a 、 K を生成する。
- ・ 暗号装置110eは、別途、乱数値 u を、復号装置120eへ送信する。

また、暗号装置110eは、乱数値 u を暗号化して送信してもよい。

(5) さらに、乱数値 u は、暗号装置110eと復号装置120eとで同じ値を得られればよい。乱数値 u の一部から構成される部分情報を第1関数部113e及び第4関数部126eで生成し、乱数値 u の残りの部分情報を暗号装置110eから復号装置120eに直接送信してもよい。

例えば、以下のように、暗号文 C と乱数値 $u2$ とを復号装置120eに送信してもよい。

- ・ $G(s)$ を生成し、 $G(s)$ から a 、 K 、 $u1$ を生成する。
- ・ 暗号装置110eは、別途、乱数値 $u2$ を、復号装置120eへ送信する。
- ・ 乱数値 u を、 $u = u1 \text{ xor } u2$ により生成する。

また、暗号装置110eは、乱数値 $u2$ を暗号化して送信してもよい。

(6) 復号装置120eは、第1暗号文 $c1$ が第4関数部126eで得られる検証値 a'' の暗号文かどうかチェックを行い、 $c1$ が a'' の暗号文であるときに共有鍵 K' を用いて共通鍵暗号文 Ci を復号しているが、実施の形態3の復号装置120dと同じチェック方法により行うとしてもよい。

すなわち、図20の処理系統図に示すように、復号装置120dと同じ復号化部123d及び比較部127dを用いて、以下のように、チェックしてもよい。

(a) 秘密鍵多項式 f を用いて第1暗号文 c_1 を復号して a' を生成する (ステップ S 2 5 2)。

(b) $s' = c_2 \text{ xor } H(a', c_1)$ を生成する (ステップ S 2 5 4)。

(c) $G(s')$ を生成し (ステップ S 2 5 5)、 $G(s')$ から a'' 、 K' 、 u' を生成する (ステップ S 2 5 6 e)。

(d) $a'' = a'$ が成立するかどうかチェックする (ステップ S 2 5 7)。成立すれば共有鍵 K' を出力する (ステップ S 2 5 8)。

また、このチェックは、第1暗号文 c_1 が復号検証値 a' の暗号文かどうかのチェックでもよい。

7. 実施の形態3及び実施の形態4のまとめ

以上説明したように、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化部とを備え、前記暗号化共有鍵データは、前記第1の暗号予備データと前記第2の暗号予備データから構成される。

また、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データと前記第1の暗号予備データを所定の処理に基づいて検証値データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化部とを備え、前記暗号化共有鍵データは、前記第1の暗号予備データと前記第2の暗号予備データから構成される。

また、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと乱数データと前記共有鍵データとに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変

換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化部とを備え、前記暗号化共有鍵データは、前記第1の暗号予備データと前記第2の暗号予備データから構成される。

また、本発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと乱数データと前記共有鍵データとに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化部と、前記検証値データと前記第1の暗号予備データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化部とを備え、前記暗号化共有鍵データは、前記第1の暗号予備データと前記第2の暗号予備データから構成される。

ここで、前記秘密数データは、ランダムに生成される乱数であるとしてもよい。

ここで、前記共有鍵導出部は、所定の処理として、一方方向性ハッシュ関数を用いるとしてもよい。

ここで、前記第1の暗号化部は、NTRU暗号方式により暗号化して前記第1の暗号予備データを生成するとしてもよい。

ここで、前記検証値変換部は、所定の処理として、一方方向性ハッシュ関数を用いるとしてもよい。

ここで、前記検証値変換部は、所定の処理として、前記検証値データをそのまま前記変換検証値データとするとしてもよい。

ここで、前記第2の暗号化部は、前記秘密数データと前記変換検証値データの排他的論理和演算を行って前記第2の暗号予備データを生成するとしてもよい。

ここで、前記第2の暗号化部は、前記秘密数データを、前記変換検証値データを暗号鍵として用いて共通鍵暗号方式により暗号化して前記第2の暗号予備データを生成するとしてもよい。

ここで、前記第2の暗号化部は、前記秘密数データに前記変換検証値データを加算して前記第2の暗号予備データを生成するとしてもよい。

ここで、前記第2の暗号化部は、前記秘密数データに前記変換検証値データを乗算して前記第2の暗号予備データを生成するとしてもよい。

ここで、前記暗号化共有鍵データは、前記第1の暗号予備データと前記第2暗号予備データのビット連結データであるとしてもよい。

また、本発明は、予め与えられた秘密鍵データに基づいて、第1の暗号予備データと第2の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力すると

有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと前記共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データと前記第１の暗号予備データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと前記共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データに基づいて、第１の暗号予備データと第２の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第１の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第１の復号化部と、前記検証値データと前記第１の暗号予備データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第２の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第２の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第1の暗号予備データと第2の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第1の復号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第2の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第2の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値検証データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化部とを備え、前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第1の暗号予備データと第2の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第1の復号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第2の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第2の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化部とを備え、前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第1の暗号予備データと第2の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第1の復号化部と、前記検証値データと前記第1の暗号予備データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第2の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第2の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値検証データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化部とを備え、前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記共有鍵データを出力する。

また、本発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第1の暗号予備データと第2の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵デ

ータを出力する共有鍵復元装置であって、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第1の復号化部と、前記検証値データと前記第1の暗号予備データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第2の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第2の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化部とを備え、前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記共有鍵データを出力する。

ここで、前記共有鍵導出部は、所定の処理として、一方方向性ハッシュ関数を用いるとしてもよい。

ここで、前記第1の復号化部は、NTRU暗号方式により復号化して検証値データを生成するとしてもよい。

ここで、前記検証値変換部は、所定の処理として、一方方向性ハッシュ関数を用いるとしてもよい。

ここで、前記検証値変換部は、所定の処理として、前記検証値データをそのまま前記変換検証値データとするとしてもよい。

ここで、前記第2の復号化部は、前記第2の暗号予備データと前記変換検証値データの排他的論理和演算を行って前記秘密数データを生成するとしてもよい。

ここで、前記第2の復号化部は、前記第2の暗号予備データを、前記変換検証値データを暗号鍵として用いて共通鍵暗号方式により復号化して前記秘密数データを生成するとしてもよい。

ここで、前記第2の復号化部は、前記第2の暗号予備データに前記変換検証値データを減算して前記秘密数データを生成するとしてもよい。

ここで、前記第2の暗号化部は、前記第2の暗号予備データを前記変換検証値データで除算して前記秘密数データを生成するとしてもよい。

また、本発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置であって、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化部と、前記平文データを前記共有鍵データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化部とを備え、前記暗号文デ

ータは、前記第1の暗号予備データと前記第2の暗号予備データと前記第3の暗号予備データから構成される。

また、本発明は、予め与えられた秘密鍵データに基づいて、第1の暗号予備データと第2の暗号予備データと第3の暗号予備データから構成される暗号文データを復号して復号文データを出力する復号装置であって、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第1の復号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記第2の暗号予備データを前記変換検証値データに基づいて復号化して秘密数データを生成する第2の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記第3の暗号予備データを前記共有鍵データに基づいて復号化して前記復号文データを生成する復号部とを備える。

また、本発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置、及び予め与えられた秘密鍵データに基づいて暗号文データを復号して復号文データを出力する復号装置からなる暗号システムである。前記暗号装置は、秘密数データを生成する秘密数データ生成部と、前記秘密数データを所定の処理に基づいて検証値データと共有鍵データに変換する共有鍵導出部と、前記検証値データを前記公開鍵データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化部と、前記検証値データを所定の処理に基づいて変換検証値データに変換する検証値変換部と、前記秘密数データを前記変換検証値データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化部と、前記平文データを前記共有鍵データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化部とを備え、前記暗号文データは、前記第1の暗号予備データと前記第2の暗号予備データと前記第3の暗号予備データから構成される。前記復号装置は、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して前記検証値データを生成する第1の復号化部と、前記検証値データを所定の処理に基づいて前記変換検証値データに変換する検証値変換部と、前記第2の暗号予備データを前記変換検証値データに基づいて復号化して前記秘密数データを生成する第2の復号化部と、前記秘密数データを所定の処理に基づいて検証値検証データと共有鍵データに変換する共有鍵導出部とを備え、前記検証値データと前記検証値検証データが一致する場合に、前記第3の暗号予備データを前記共有鍵データに基づいて復号化して前記復号文データを生成する復号部とを備える。

以上に説明したように、本発明は、従来システムにおける問題点を鑑みて行われたもので、暗号システムにおいて、NTRU暗号を適用できる鍵カプセル化メカニズムを構成することで、暗号装置と復号装置との間でNTRU暗号を用いて鍵配送が行えるようになる。

以上により、従来技術では達成できなかった暗号システムを提供することができ、その価

値は大きい。

8. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

(1) 暗号装置が、インターネットを介して、各暗号文を復号装置へ送信する代わりに、暗号装置は、各暗号文をDVDなどの記録媒体に書き込み、復号装置は、記録媒体から各暗号文を読み出すとしてもよい。

(2) 本発明で用いるNTRU暗号は、非特許文献2に記載の方式以外に、E E S S (Efficient Embedded Security Standard) 方式のNTRU暗号であってもよい。E E S S方式のNTRU暗号については、“EES;Consortium for Efficient Embedded Security, Efficient Embedded Security Standards #1:Implementation Aspects of NTRU Encrypt and NTRU Sign, Version 2.0,” available at <http://ceesstandards.org>, May 2003.に詳細に記述されている。このため、ここではその詳細については説明を省くが、以下に簡単に説明する。

E E S S方式のNTRU暗号では、乱数多項式 r は、 d 個の係数が1であり、 $(N-d)$ 個の係数が0である多項式、もしくはこのような複数の多項式を用いて計算される多項式である。従って、上記の実施の形態において、乱数多項式 r を生成する際に、このような多項式となるように生成すれば、NTRU暗号の代わりにE E S S方式のNTRU暗号を用いることができ、同様の効果が得られる。

(3) コンテンツ配信システムは、次に示すように構成してもよい。

コンテンツ配信システムは、コンテンツサーバ装置と暗号装置と放送装置と受信装置と復号装置と再生装置とモニタとから構成されている。

暗号装置と復号装置とは、コンテンツ配信システム10の暗号装置110と復号装置120とに対応している。

コンテンツサーバ装置と暗号装置とは、専用回線を介して接続されており、コンテンツサーバ装置は、映像と音声から構成される映画などのコンテンツを専用回線を介して暗号装置へ送信する。暗号装置と放送装置とは、専用回線を介して接続されている。暗号装置は、各暗号文を放送装置へ送信し、放送装置は、各暗号文を多重化し、デジタル放送波に乗せて放送する。

受信装置と復号装置とは、接続されており、復号装置と再生装置とは、接続されている。受信装置は、デジタル放送波を受信し、受信したデジタル放送波から各暗号文を抽出し、抽出した各暗号文を復号装置へ送信する。復号装置は、各暗号文を受け取り、受け取った各暗号文を用いて、再生コンテンツを生成し、生成した再生コンテンツを再生装置へ出力する。再生装置は、復号装置及びスピーカを内蔵するモニタに接続されている。再生装置は、再生

コンテンツを受け取り、受け取った再生コンテンツから映像信号及び音声信号を生成し、モニタは、映像を表示し、音声を出力する。

(4) コンテンツサーバ装置と暗号装置とは、一体となった装置から構成されているとしてもよい。また、復号装置と再生装置とは、一体となった装置から構成されているとしてもよい。

(5) 上記の各実施の形態において、メモリカード160は、予め公開鍵多項式 h を記憶しており、メモリカード170は、予め秘密鍵多項式 f 及び公開鍵多項式 h を記憶しており、暗号装置110及び復号装置120は、メモリカード160及びメモリカード170から、それぞれ公開鍵多項式、秘密鍵多項式を取得するとしているが、これには限定されない。

暗号装置110は、予め公開鍵多項式を記憶しており、復号装置120は、予め公開鍵多項式及び秘密鍵多項式を記憶しているとしてもよい。

また、鍵管理装置は、秘密鍵多項式及び公開鍵多項式を生成し、生成した秘密鍵多項式及び公開鍵多項式を秘密にかつ安全に復号装置120へ送信し、生成した公開鍵多項式を暗号装置110へ送信するとしてもよい。

(6) コンテンツ配信システムにおいて配信されるコンテンツは、映像と音声とからなる映画などのコンテンツには、限定されない。動画像、静止画像、音声、音楽、文書、小説、DBソフトにより生成されるデータベース、表計算ソフトにより生成される電子的な表データ、コンピュータプログラム、その他コンピュータ用データなどであってもよい。

また、前記コンテンツは、上記のような著作物ではなく、暗号化及び復号化、デジタル署名及び署名検証などに用いる鍵情報であるとしてもよい。

例えば、上記の各実施の形態により示されるようにして、暗号装置及び復号装置は、共有鍵を共有し、暗号装置は、コンテンツ鍵を共有鍵を用いて暗号化して暗号化コンテンツ鍵を生成し、コンテンツをコンテンツ鍵を用いて暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツ鍵と生成した暗号化コンテンツとを復号装置に送信する。復号装置は、暗号化コンテンツ鍵と暗号化コンテンツとを受信し、共有鍵を用いて、暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、生成したコンテンツ鍵を用いて暗号化コンテンツを復号してコンテンツを生成するとしてもよい。

(7) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記

コンピュータプログラム又は前記デジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(8) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

Although the present invention has been fully described by way of examples with reference to the accompanying drawings, it is to be noted that various changes and modifications will be apparent to those skilled in the art. Therefore, unless otherwise such changes and modifications depart from the scope of the present invention, they should be construed as being included therein.

産業上の利用の可能性

上記において説明したコンテンツ配布システムは、コンテンツ供給者から利用者に対して、音楽、映画、小説などのデジタル化された著作物を供給する産業において、経営的、反復的かつ継続的に使用される。また、コンテンツ配布システムを構成する暗号装置及び復号装置は、電化製品などを製造する電機機器産業において、製造され、販売される。

特に、デジタル化された著作物を、DVDなどの記録媒体に格納して市場に流通させることにより、ネットワークを介して流通させることにより、又は放送により、供給する産業において好適である。

【What is claimed is:】

1. 第3者に知られることなく共有鍵を生成する共有鍵生成装置及び共有鍵復元装置から構成される鍵共有システムであって、
前記共有鍵生成装置は、
シード値を生成するシード値生成手段と、
生成された前記シード値から検証値及び共有鍵を生成する第1共有鍵生成手段と、
生成された前記検証値を暗号化して、第1暗号化情報を生成する第1暗号化手段と、
生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第2暗号化情報を生成する第2暗号化手段と、
生成された前記第1暗号化情報及び前記第2暗号化情報を送信する送信手段とを備え、
前記共有鍵復元装置は、
前記第1暗号化情報及び前記第2暗号化情報を受信する受信手段と、
受信された前記第1暗号化情報を復号して第1復号検証値を生成する第1復号手段と、
生成された前記第1復号検証値に基づいて、受信された前記第2暗号化情報を復号して、
復号シード値を生成する第2復号手段と、
前記第1共有鍵生成手段と同一の方法により、生成された前記復号シード値から第2復号検証値及び復号共有鍵を生成する第2共有鍵生成手段と、
生成された前記第1復号検証値及び前記第2復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断手段と、
出力すると判断される場合に、生成された前記復号共有鍵を出力する出力手段とを備えることを特徴とする鍵共有システム。
2. 前記共有鍵生成装置は、さらに、
コンテンツを取得する取得手段と、
生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成する暗号化手段とを備え、
前記送信手段は、さらに、生成された前記暗号化コンテンツを送信し、
前記受信手段は、さらに、前記暗号化コンテンツを受信し、
前記共有鍵復元装置は、さらに、
出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成する復号手段と、
生成された復号コンテンツを出力する出力手段とを備えることを特徴とする請求の範囲1に記載の鍵共有システム。
3. 第3者に知られることなく共有鍵を相手の装置へ伝える共有鍵生成装置であって、
シード値を生成するシード値生成手段と、

- 生成された前記シード値から検証値及び共有鍵を生成する共有鍵生成手段と、
生成された前記検証値を暗号化して、第1暗号化情報を生成する第1暗号化手段と、
生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第2暗号化情報を生成する第2暗号化手段と、
生成された前記第1暗号化情報及び前記第2暗号化情報を送信する送信手段と
を備えることを特徴とする共有鍵生成装置。
4. 前記シード値生成手段は、乱数を生成し、生成した乱数を前記シード値とすることにより、前記シード値を生成する
ことを特徴とする請求の範囲3に記載の共有鍵生成装置。
5. 前記共有鍵生成手段は、前記シード値に一方方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値及び前記共有鍵を生成する
ことを特徴とする請求の範囲3に記載の共有鍵生成装置。
6. 前記共有鍵生成手段は、前記シード値に、前記一方方向性関数として、ハッシュ関数を施して前記関数値を生成する
ことを特徴とする請求の範囲5に記載の共有鍵生成装置。
7. 前記共有鍵生成手段は、生成された前記関数値の一部を前記検証値とし、他の一部を前記共有鍵とすることにより、前記検証値及び前記共有鍵を生成する
ことを特徴とする請求の範囲5に記載の共有鍵生成装置。
8. 前記共有鍵生成手段は、前記シード値に一方方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値、前記共有鍵及びブラインド値を生成する
ことを特徴とする請求の範囲3に記載の共有鍵生成装置。
9. 前記第1暗号化手段は、
公開鍵を取得する公開鍵取得部と、
取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第1暗号化情報を生成する公開鍵暗号化部と含む
ことを特徴とする請求の範囲8に記載の共有鍵生成装置。
10. 前記公開鍵暗号化アルゴリズムは、NTRU暗号方式によるものであり、
前記公開鍵取得部は、前記公開鍵として、NTRU暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し
前記公開鍵暗号化部は、前記検証値から検証値多項式を生成し、前記ブラインド値からブラインド値多項式を生成し、NTRU暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第1暗号化情報を生成する
ことを特徴とする請求の範囲9に記載の共有鍵生成装置。

11. 前記第1暗号化手段は、
公開鍵を取得する公開鍵取得部と、
取得された前記公開鍵を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第1暗号化情報を生成する公開鍵暗号化部を含む
ことを特徴とする請求の範囲3に記載の共有鍵生成装置。
12. 前記公開鍵暗号化アルゴリズムは、NTRU暗号方式によるものであり、
前記公開鍵取得部は、前記公開鍵として、NTRU暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し
前記公開鍵暗号化部は、前記検証値から検証値多項式を生成し、ブラインド値を生成し、生成した前記ブラインド値からブラインド値多項式を生成し、NTRU暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第1暗号化情報を生成する
ことを特徴とする請求の範囲11に記載の共有鍵生成装置。
13. 前記第2暗号化手段は、前記検証値に一方方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第2暗号化情報を生成する
ことを特徴とする請求の範囲3に記載の共有鍵生成装置。
14. 前記第2暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第2暗号化情報を生成する
ことを特徴とする請求の範囲13に記載の共有鍵生成装置。
15. 前記第2暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして共通鍵暗号化アルゴリズムを施すことにより、前記第2暗号化情報を生成する
ことを特徴とする請求の範囲13に記載の共有鍵生成装置。
16. 前記第2暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして加算を施すことにより、前記第2暗号化情報を生成する
ことを特徴とする請求の範囲13に記載の共有鍵生成装置。
17. 前記第2暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして乗算を施すことにより、前記第2暗号化情報を生成する
ことを特徴とする請求の範囲13に記載の共有鍵生成装置。
18. 前記第2暗号化手段は、前記検証値に、前記一方方向性関数としてハッシュ関数を施して前記関数値を生成する
ことを特徴とする請求の範囲13に記載の共有鍵生成装置。
19. 前記第2暗号化手段は、前記検証値を用いて、前記シード値に暗号化アルゴリズムを施

して第2暗号化情報を生成する

ことを特徴とする請求の範囲3に記載の共有鍵生成装置。

20. 前記第2暗号化手段は、前記検証値及び前記第1暗号化情報を用いて、前記シード値を暗号化する

ことを特徴とする請求の範囲3に記載の共有鍵生成装置。

21. 前記第2暗号化手段は、前記検証値及び前記第1暗号化情報に一方方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第2暗号化情報を生成する

ことを特徴とする請求の範囲20に記載の共有鍵生成装置。

22. 前記第2暗号化手段は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第2暗号化情報を生成する

ことを特徴とする請求の範囲21に記載の共有鍵生成装置。

23. 前記共有鍵生成装置は、さらに、

コンテンツを取得する取得手段と、

生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成する暗号化手段とを備え、

前記送信手段は、さらに、生成された前記暗号化コンテンツを送信する

ことを特徴とする請求の範囲3に記載の共有鍵生成装置。

24. 第3者に知られることなく共有鍵生成装置から共有鍵を受け取る共有鍵復元装置であって、

前記共有鍵生成装置は、シード値を生成し、生成された前記シード値から検証値及び共有鍵を生成し、生成された前記検証値を暗号化して、第1暗号化情報を生成し、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第2暗号化情報を生成し、生成された前記第1暗号化情報及び前記第2暗号化情報を送信し、

前記共有鍵復元装置は、

前記第1暗号化情報及び前記第2暗号化情報を受信する受信手段と、

受信された前記第1暗号化情報を復号して第1復号検証値を生成する第1復号手段と、

生成された前記第1復号検証値に基づいて、受信された前記第2暗号化情報を復号して、復号シード値を生成する第2復号手段と、

前記共有鍵生成装置と同一の方法により、生成された前記復号シード値から第2復号検証値及び復号共有鍵を生成する共有鍵生成手段と、

生成された前記第1復号検証値及び前記第2復号検証値に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断手段と、

出力すると判断される場合に、生成された前記復号共有鍵を出力する出力手段と

を備えることを特徴とする共有鍵復元装置。

25. 前記共有鍵生成装置は、公開鍵を取得し、取得された前記公開鍵を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第1暗号化情報を生成し、

前記第1復号手段は、

前記公開鍵に対応する秘密鍵を取得する秘密鍵取得部と、

取得された前記秘密鍵を用いて、受信した前記第1暗号化情報に、前記公開鍵暗号化アルゴリズムに対応する公開鍵復号アルゴリズムを施して前記第1復号検証値を生成する公開鍵復号部を含む

ことを特徴とする請求の範囲24に記載の共有鍵復元装置。

26. 前記公開鍵暗号化アルゴリズム及び前記公開鍵復号アルゴリズムは、NTRU暗号方式によるものであり、

前記共有鍵生成装置は、前記公開鍵として、NTRU暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記検証値から検証値多項式を生成し、ブラインド値を生成し、生成した前記ブラインド値からブラインド値多項式を生成し、NTRU暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第1暗号化情報を生成し、

前記受信手段は、多項式としての前記第1暗号化情報を受信し、

前記秘密鍵取得部は、前記秘密鍵として、NTRU暗号方式の鍵生成アルゴリズムにより生成された秘密鍵多項式を取得し、

前記公開鍵復号部は、NTRU暗号方式の前記暗号化アルゴリズムに対応する復号アルゴリズムにより、前記秘密鍵多項式を鍵として用いて、多項式としての前記第1暗号化情報を復号して、復号検証値多項式を生成し、生成した前記復号検証値多項式から前記第1復号検証値を生成する

ことを特徴とする請求の範囲25に記載の共有鍵復元装置。

27. 前記共有鍵生成装置は、前記検証値に一方方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第2暗号化情報を生成し、

前記第2復号手段は、生成された前記第1復号検証値に、前記一方方向性関数を施して復号関数値を生成し、生成した前記復号関数値を用いて、受信された前記第2暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して前記復号シード値を生成する

ことを特徴とする請求の範囲24に記載の共有鍵復元装置。

28. 前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第2暗号化情報を生成し、

前記第2復号手段は、生成した前記復号関数値と前記第2暗号化情報とに、前記復号アルゴリズムとして排他的論理和を施すことにより、前記復号シード値を生成する

ことを特徴とする請求の範囲27に記載の共有鍵復元装置。

29. 前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして共通鍵暗号化アルゴリズムを施すことにより、前記第2暗号化情報を生成し、

前記第2復号手段は、生成した前記復号関数値と前記第2暗号化情報とに、前記復号アルゴリズムとして、前記共通鍵暗号化アルゴリズムに対応する共通鍵復号アルゴリズムを施すことにより、前記復号シード値を生成する

ことを特徴とする請求の範囲27に記載の共有鍵復元装置。

30. 前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして加算を施すことにより、前記第2暗号化情報を生成し、

前記第2復号手段は、生成した前記復号関数値と前記第2暗号化情報とに、前記復号アルゴリズムとして、減算を施すことにより、前記復号シード値を生成する

ことを特徴とする請求の範囲27に記載の共有鍵復元装置。

31. 前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして乗算を施すことにより、前記第2暗号化情報を生成し、

前記第2復号手段は、生成した前記復号関数値と前記第2暗号化情報とに、前記復号アルゴリズムとして、除算を施すことにより、前記復号シード値を生成する

ことを特徴とする請求の範囲27に記載の共有鍵復元装置。

32. 前記共有鍵生成装置は、前記検証値に、前記一方向性関数としてハッシュ関数を施して前記関数値を生成し、

前記第2復号手段は、生成された前記第1復号検証値に、前記一方向性関数として前記ハッシュ関数を施して前記復号関数値を生成する

ことを特徴とする請求の範囲27に記載の共有鍵復元装置。

33. 前記共有鍵生成装置は、前記検証値を用いて、前記シード値に暗号化アルゴリズムを施して第2暗号化情報を生成し、

前記第2復号手段は、生成された前記第1復号検証値を用いて、前記第2暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して、前記復号シード値を生成する

ことを特徴とする請求の範囲24に記載の共有鍵復元装置。

34. 前記共有鍵生成装置は、前記検証値及び前記第1暗号化情報を用いて、前記シード値を暗号化し、

前記第2復号手段は、生成された前記第1復号検証値及び受信された前記第1暗号化情報を用いて、前記第2暗号化情報を復号して前記復号シード値を生成する

ことを特徴とする請求の範囲 24 に記載の共有鍵復元装置。

35. 前記共有鍵生成装置は、前記検証値及び前記第 1 暗号化情報に一方方向性関数を施して関数値を生成し、生成した前記関数値を用いて、前記シード値に暗号化アルゴリズムを施して前記第 2 暗号化情報を生成し、

前記第 2 復号手段は、前記第 1 復号検証値及び前記第 1 暗号化情報に前記一方方向性関数を施して復号関数値を生成し、生成した前記復号関数値を用いて、前記第 2 暗号化情報に、前記暗号化アルゴリズムに対応する復号アルゴリズムを施して、前記復号シード値を生成する

ことを特徴とする請求の範囲 34 に記載の共有鍵復元装置。

36. 前記共有鍵生成装置は、生成した前記関数値と前記シード値とに、前記暗号化アルゴリズムとして排他的論理和を施すことにより、前記第 2 暗号化情報を生成し、

前記第 2 復号手段は、前記復号関数値及び前記第 2 暗号化情報に、前記復号アルゴリズムとして、排他的論理和を施すことにより、前記復号シード値を生成する

ことを特徴とする請求の範囲 35 に記載の共有鍵復元装置。

37. 前記共有鍵生成装置は、前記シード値に一方方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値及び前記共有鍵を生成し、

前記共有鍵生成手段は、生成された前記復号シード値に、前記一方方向性関数を施して復号関数値を生成し、生成した前記復号関数値から前記第 2 復号検証値及び前記復号共有鍵を生成する

ことを特徴とする請求の範囲 24 に記載の共有鍵復元装置。

38. 前記共有鍵生成装置は、前記シード値に、前記一方方向性関数として、ハッシュ関数を施して前記関数値を生成し、

前記共有鍵生成手段は、生成された前記復号シード値に、前記一方方向性関数として、前記ハッシュ関数を施して前記復号関数値を生成する

ことを特徴とする請求の範囲 37 に記載の共有鍵復元装置。

39. 前記共有鍵生成装置は、生成された前記関数値の一部を前記検証値とし、他の一部を前記共有鍵とすることにより、前記検証値及び前記共有鍵を生成し、

前記共有鍵生成手段は、生成された前記復号関数値の一部を前記第 2 復号検証値とし、他の一部を前記復号共有鍵とすることにより、前記第 2 復号検証値及び前記復号共有鍵を生成する

ことを特徴とする請求の範囲 37 に記載の共有鍵復元装置。

40. 前記共有鍵生成装置は、前記シード値に一方方向性関数を施して関数値を生成し、生成した前記関数値から前記検証値、前記共有鍵及びブラインド値を生成し、公開鍵を取得し、取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第 1 暗号化情報を生成し、

前記共有鍵生成手段は、生成された前記復号シード値に、前記一方向性関数を施して復号関数値を生成し、生成した前記復号関数値から前記第2復号検証値、前記復号共有鍵及び復号ブラインド値を生成する

ことを特徴とする請求の範囲24に記載の共有鍵復元装置。

41. 前記共有鍵生成装置は、公開鍵を取得し、取得された前記公開鍵及び生成された前記ブラインド値を用いて、前記検証値に公開鍵暗号化アルゴリズムを施して前記第1暗号化情報を生成し、

前記判断手段は、前記第1復号検証値及び前記第2復号検証値に基づく前記判断に代えて、前記公開鍵を取得する公開鍵取得部と、

取得された前記公開鍵及び生成された前記復号ブラインド値を用いて、生成された前記第1復号検証値又は前記第2復号検証値に前記公開鍵暗号化アルゴリズムを施して再暗号化情報を生成する再暗号化部と、

受信された前記第1暗号化情報及び生成された前記再暗号化情報に基づいて、生成された前記復号共有鍵を出力するか否かを判断する判断部とを備える

ことを特徴とする請求の範囲40に記載の共有鍵復元装置。

42. 前記判断部は、前記第1暗号化情報と前記再暗号化情報とを比較し、前記第1暗号化情報と前記再暗号化情報とが一致する場合に、前記復号共有鍵を出力すると判断する

ことを特徴とする請求の範囲41に記載の共有鍵復元装置。

43. 前記公開鍵暗号化アルゴリズムは、NTRU暗号方式によるものであり、

前記共有鍵生成装置は、前記公開鍵として、NTRU暗号方式の鍵生成アルゴリズムにより生成された公開鍵多項式を取得し、前記検証値から検証値多項式を生成し、前記ブラインド値からブラインド値多項式を生成し、NTRU暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記検証値多項式を攪乱するために前記ブラインド値多項式を用いて、前記検証値多項式を暗号化して、多項式としての前記第1暗号化情報を生成し、

前記公開鍵取得部は、前記公開鍵多項式を取得し、

前記再暗号化部は、前記第2復号検証値から復号検証値多項式を生成し、前記復号ブラインド値から復号ブラインド値多項式を生成し、NTRU暗号方式の暗号化アルゴリズムにより、前記公開鍵多項式を鍵として用い、前記復号検証値多項式を攪乱するために前記復号ブラインド値多項式を用いて、前記復号検証値多項式を暗号化して、多項式としての前記再暗号化情報を生成する

ことを特徴とする請求の範囲41に記載の共有鍵復元装置。

44. 前記判断手段は、前記第1復号検証値と前記第2復号検証値とを比較し、一致する場合に、前記復号共有鍵を出力すると判断する

ことを特徴とする請求の範囲24に記載の共有鍵復元装置。

45. 前記共有鍵生成装置は、さらに、コンテンツを取得し、生成された前記共有鍵を用いて、取得されたコンテンツを暗号化して、暗号化コンテンツを生成し、生成された前記暗号化コンテンツを送信し、

前記受信手段は、さらに、前記暗号化コンテンツを受信し、

前記共有鍵復元装置は、さらに、

出力された前記復号共有鍵を用いて、受信された前記暗号化コンテンツを復号して、復号コンテンツを生成する復号手段と、

生成された復号コンテンツを出力する出力手段とを備える

ことを特徴とする請求の範囲24に記載の共有鍵復元装置。

46. 第3者に知られることなく共有鍵を相手の装置へ伝える共有鍵生成装置で用いられる共有鍵生成方法であって、

シード値を生成するシード値生成ステップと、

生成された前記シード値から検証値及び共有鍵を生成する共有鍵生成ステップと、

生成された前記検証値を暗号化して、第1暗号化情報を生成する第1暗号化ステップと、

生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第2暗号化情報を生成する第2暗号化ステップと、

生成された前記第1暗号化情報及び前記第2暗号化情報を送信する送信ステップと

を含むことを特徴とする共有鍵生成方法。

47. 第3者に知られることなく共有鍵を相手の装置へ伝える共有鍵生成装置で用いられる共有鍵生成プログラムであって、

シード値を生成するシード値生成ステップと、

生成された前記シード値から検証値及び共有鍵を生成する共有鍵生成ステップと、

生成された前記検証値を暗号化して、第1暗号化情報を生成する第1暗号化ステップと、

生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第2暗号化情報を生成する第2暗号化ステップと、

生成された前記第1暗号化情報及び前記第2暗号化情報を送信する送信ステップと

を含むことを特徴とする共有鍵生成プログラム。

48. 前記共有鍵生成プログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求の範囲48に記載の共有鍵生成プログラム。

49. 第3者に知られることなく共有鍵生成装置から共有鍵を受け取る共有鍵復元装置で用いられる共有鍵復元方法であって、

前記共有鍵生成装置は、シード値を生成し、生成された前記シード値から検証値及び共有鍵を生成し、生成された前記検証値を暗号化して、第1暗号化情報を生成し、生成された前記検証値に基づいて、生成された前記シード値を暗号化して、第2暗号化情報を生成し、生

成された前記第 1 暗号化情報及び前記第 2 暗号化情報を送信し、

前記共有鍵復元方法は、

前記第 1 暗号化情報及び前記第 2 暗号化情報を受信する受信ステップと、

受信された前記第 1 暗号化情報を復号して第 1 復号検証値を生成する第 1 復号ステップと、

生成された前記第 1 復号検証値に基づいて、受信された前記第 2 暗号化情報を復号して、
復号シード値を生成する第 2 復号ステップと、

前記共有鍵生成装置と同一の方法により、生成された前記復号シード値から第 2 復号検証
値及び復号共有鍵を生成する共有鍵生成ステップと、

生成された前記第 1 復号検証値及び前記第 2 復号検証値に基づいて、生成された前記復号
共有鍵を出力するか否かを判断する判断ステップと、

出力すると判断される場合に、生成された前記復号共有鍵を出力する出力ステップと
を含むことを特徴とする共有鍵復元方法。

50. 第 3 者に知られることなく共有鍵生成装置から共有鍵を受け取る共有鍵復元装置で用い
られる共有鍵復元プログラムであって、

前記共有鍵生成装置は、シード値を生成し、生成された前記シード値から検証値及び共有
鍵を生成し、生成された前記検証値を暗号化して、第 1 暗号化情報を生成し、生成された前
記検証値に基づいて、生成された前記シード値を暗号化して、第 2 暗号化情報を生成し、生
成された前記第 1 暗号化情報及び前記第 2 暗号化情報を送信し、

前記共有鍵復元プログラムは、

前記第 1 暗号化情報及び前記第 2 暗号化情報を受信する受信ステップと、

受信された前記第 1 暗号化情報を復号して第 1 復号検証値を生成する第 1 復号ステップと、

生成された前記第 1 復号検証値に基づいて、受信された前記第 2 暗号化情報を復号して、
復号シード値を生成する第 2 復号ステップと、

前記共有鍵生成装置と同一の方法により、生成された前記復号シード値から第 2 復号検証
値及び復号共有鍵を生成する共有鍵生成ステップと、

生成された前記第 1 復号検証値及び前記第 2 復号検証値に基づいて、生成された前記復号
共有鍵を出力するか否かを判断する判断ステップと、

出力すると判断される場合に、生成された前記復号共有鍵を出力する出力ステップと
を含むことを特徴とする共有鍵復元プログラム。

51. 前記共有鍵復元プログラムは、コンピュータ読み取り可能な記録媒体に記録されている
ことを特徴とする請求の範囲 50 に記載の共有鍵復元プログラム。

【ABSTRACT OF DISCLOSURE】

暗号装置と復号装置との間で異なる鍵の導出を防止するコンテンツ配信システムを提供する。

暗号装置 110d の乱数生成部 112d は、乱数 s を生成し、第 1 関数部 113d は、乱数 s の関数値 $G(s)$ を生成し、関数値 $G(s)$ から検証値 a と共有鍵 K を生成し、暗号化部 114d は、公開鍵多項式 h を用いて検証値 a の第 1 暗号文 $c1$ を生成し、第 2 関数部 115d は、検証値 a と第 1 暗号文 $c1$ の関数値 $H(a,c1)$ を生成し、乱数マスク部 116d は、第 2 暗号文 $c2=s \text{ xor } H(a,c1)$ を生成する。

復号装置 120d の復号化部 123d は、秘密鍵多項式 f を用いて、第 1 暗号文 $c1$ を復号して復号検証値 a' を生成し、第 3 関数部 124d は、検証値 a' と第 1 暗号文 $c1$ の関数値 $H(a',c1)$ を生成し、乱数マスク除去部 125d は、復号乱数 $s'=c2 \text{ xor } H(a',c1)$ を生成し、第 4 関数部 126d は、復号乱数 s' のハッシュ関数値 $G(s')$ を生成し、関数値 $G(s')$ から検証値 a'' と共有鍵 K' を生成し、比較部 127d は、復号検証値 a' と検証値 a'' が等しければ、共有鍵 K' を出力する。

(選択図 図 16)